



WESTERN MULTIPLEX CORPORATION  

---

Installation and Maintenance Manual

# **Tsunami**<sup>TM</sup>

Base Station Unit

Multipoint  
SS



Revisions:

September 2001

Draft

October

FCC submittal

December

Released for review

WESTERN MULTIPLEX CORPORATION

# Tsunami Point-to-Multipoint

---

© 2001

Western Multiplex Corporation  
1196 Borregas Avenue  
Sunnyvale, California 94089 USA  
Phone +1 408 542 5200 • Fax +1 408 542 5300

<http://www.wmux.com>

<ftp://ftp.wmux.com/products/>

---

**NOTICE: CAREFULLY READ THE FOLLOWING LIMITED WARRANTY AND LIMITATION OF LIABILITY (THE “LIMITED WARRANTY”). BY USING THE WESTERN MULTIPLEX EQUIPMENT INCLUDED WITH THIS LIMITED WARRANTY, YOU AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS LIMITED WARRANTY. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, RETURN THE WESTERN MULTIPLEX EQUIPMENT TO WHERE IT WAS PURCHASED OR LEASED WITHIN THIRTY (30) DAYS OF RECEIPT FOR A FULL REFUND.**

## **1. LIMITED EQUIPMENT WARRANTY**

- 1.1 For the applicable Warranty Period (as defined in Paragraph 1.2 below) Western Multiplex warrants that the hardware manufactured by Western Multiplex and initially purchased or leased from one of Western Multiplex’s authorized resellers or distributors by the original end-user (“you”) for your personal use and not for resale (the “Equipment”) (a) substantially conforms to the specifications contained in the most recent version of the manual for the model of the Equipment purchased or leased by you (the “Equipment Specifications”) and (b) is free from defects in materials and workmanship. This Limited Warranty only applies to the Equipment and its preloaded firmware. This Limited Warranty does not apply to any software (or its associated documentation), whether preloaded with the Equipment, installed subsequently or otherwise (“Software”), nor does it apply to any firmware revision that is not originally preloaded on the Equipment at the time the Equipment is purchased or leased. The Software is licensed to you pursuant to the software license agreement that accompanied the Software and is subject to the terms, including the limited warranty and limitation of liability, contained in that license agreement. Western Multiplex has no obligation to repair or replace Software under this Limited Warranty.
- 1.2 This Limited Warranty shall start on the date that the Equipment is first shipped to you (the “Shipping Date”) and shall end:
  - (a) for all unlicensed radio products which are point-to-multi-point products, one (1) year after the Shipping Date;
  - (b) for all accessories, one (1) year after the Shipping Date; and
  - (c) for all unlicensed radio products (except point-to-multi-point products) and for all licensed digital microwave radio products, two (2) years after the Shipping Date (in each case, the “Warranty Period”).
- 1.3 Nothing in this Limited Warranty affects any statutory rights of consumers that cannot be waived or limited by contract.

## **2. LIMITED WARRANTY EXCLUSIONS AND LIMITATIONS.**

- 2.1 The Limited Warranty covers customary and intended usage only.
- 2.2 Western Multiplex does not warrant, and is not responsible for damage, defect or failure caused by any of the following:
  - (a) Any part of the Equipment having been modified, adapted, repaired, or improperly installed, operated, maintained, stored, transported or relocated by any person other than Western Multiplex personnel or a Western Multiplex authorized service agent;
  - (b) External causes, including electrical stress or lightning, interference caused by other radios or other sources, unsuitable physical or operating environment and use in conjunction with incompatible equipment or accessories;
  - (c) Cosmetic damage, including all damage to the surface of the Equipment;

- (d) Acts of God, fires, floods, wars, terrorist acts, sabotage, civil unrest, labor disputes or similar events, actions or hazards; and
  - (e) Accidents, negligence, neglect, mishandling, abuse or misuse, other than by Western Multiplex personnel or a Western Multiplex authorized service agent.
- 2.3 The Limited Warranty does not apply to the following parts of the Equipment, which are not manufactured by Western Multiplex, but which may be otherwise covered by an original manufacturer's warranty:
  - (a) antenna systems, including coaxial cable, wave guide, connectors, flex sections, mounts, and other parts of the antenna system and installation materials;
  - (b) rack mounted equipment, which is not manufactured by Western Multiplex but which may be assembled, wired and tested at Western Multiplex's factory or supplied as part of a system, including orderwire items, channel banks, multiplexers, fuse/alarm panels and remote alarm items; and
  - (c) all equipment which is not included in Western Multiplex's specifications.
- 2.4 Unless otherwise specified, equipment not manufactured by Western Multiplex is provided "AS IS" AND WITHOUT WARRANTIES OF ANY KIND. Please refer to the original manufacturer's warranty, if any.
- 2.5 Any technical or other support provided for the Equipment by Western Multiplex, such as telephone assistance or assistance regarding installation, is provided "AS IS" AND WITHOUT WARRANTIES OF ANY KIND.

### **3. REPLACEMENT, REPAIR AND RETURN PROCESSES.**

- 3.1 To request service under the Limited Warranty:
  - (a) You must, within the applicable Warranty Period, promptly notify Western Multiplex of the problem with the Equipment, provide the serial number of the Equipment, and provide your contact information during business hours, by contacting Western Multiplex by telephone at 408-542-5390, by e-mail at support@wmux.com, or by mail to Support, Western Multiplex Corporation, 1196 Borregas Avenue, Sunnyvale, California 94089, during the business hours of 8:00 a.m. to 5:00 p.m., Pacific Time, Monday through Friday, excluding holidays. This notice is effective when received by Western Multiplex during the business hours referenced above.
  - (b) Western Multiplex shall, at its sole option, either resolve the problem over the telephone or provide you with a returned materials authorization number ("RMA Number") and the address of the location to which you may ship the Equipment at issue.
  - (c) If the problem is not resolved over the telephone, and Western Multiplex gives you an RMA Number, you must, within ten (10) business days of your receipt of an RMA Number if you are located within the borders of the United States and within thirty (30) days of your receipt of an RMA Number if you are located beyond the borders of the United States, at your cost, ship the Equipment to the location specified by Western Multiplex. The Equipment must be shipped in its original or equivalent packaging. You must also attach a label to each item of Equipment you are returning, which must include the following information: the RMA Number, a description of the problem, your return address and a telephone number where you can be reached during business hours. You must also include with the Equipment a dated proof of original purchase. YOU ARE RESPONSIBLE

FOR ALL EQUIPMENT UNTIL WESTERN MULTIPLEX RECEIVES IT, AND YOU ARE RESPONSIBLE FOR ALL SHIPPING, HANDLING AND INSURANCE CHARGES, WHICH MUST BE PREPAID.

- (d) Western Multiplex is not responsible for Equipment received without an RMA Number and may reject the return of such Equipment. Western Multiplex is also not responsible for any of your confidential, proprietary or other information or data contained in Equipment you return to Western Multiplex. You should remove any such information or data from the Equipment prior to making any return to Western Multiplex.
  - (e) The replacement or repair of Equipment in locations outside of the United States may vary depending on your location.
  - (f) FAILURE TO FOLLOW THE PROCEDURES FOR RETURNS LISTED ABOVE MAY VOID THE LIMITED WARRANTY.
- 3.2 If the Equipment does not function as warranted, as determined by Western Multiplex in its sole discretion, Western Multiplex shall either repair or replace the returned Equipment at its sole option.
- (a) The replacement item may be new or refurbished. All parts removed from repaired Equipment and all returned Equipment that is replaced by Western Multiplex become the property of Western Multiplex.
  - (b) Western Multiplex shall, at its cost (which shall not include international customs, freight forwarding, or associated fees) ship the repaired or replacement Equipment to any destination, by carrier and method of delivery chosen by Western Multiplex, in its sole discretion. Western Multiplex will not pay, and you will be solely responsible for, any international customs, freight forwarding, or other associated fees related to such shipment. If you request some other form of conveyance, such as express shipping, you must pay the cost of return shipment.
- 3.3 Equipment which is repaired or replaced by Western Multiplex under this Limited Warranty shall be covered under all of the provisions of this Limited Warranty for the remainder of the applicable Warranty Period or ninety (90) days from the date of shipment of the repaired or replacement Equipment, whichever period is longer.

#### 4. LIMITATIONS OF RIGHTS AND DISCLAIMER OF OTHER WARRANTIES

- 4.1 THE LIMITED WARRANTY CONTAINS LIMITATIONS ON YOUR RIGHTS AND REMEDIES AGAINST WESTERN MULTIPLEX. YOU ACKNOWLEDGE HAVING READ, UNDERSTOOD AND AGREED TO THOSE LIMITATIONS.
- 4.2 Western Multiplex does not warrant that the functions contained in the Equipment will meet your requirements or that any Equipment's operation will be uninterrupted or error free. REPAIR OR REPLACEMENT OF THE EQUIPMENT AS PROVIDED HEREIN IS THE EXCLUSIVE REMEDY AVAILABLE TO YOU, AND IS PROVIDED IN LIEU OF ALL OTHER WARRANTIES, WHETHER ORAL OR WRITTEN, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. ALL OTHER WARRANTIES ARE EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW AND EXCEPT FOR THE LIMITED WARRANTY PROVIDED HEREIN, THE EQUIPMENT IS PROVIDED "AS IS". No

dealer, agent, or employee is authorized to make any modification, extension, or addition to the Limited Warranty.

## **5. LIMITATION OF LIABILITY**

- 5.1 WESTERN MULTIPLEX SHALL NOT BE LIABLE TO YOU FOR INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS) OF ANY KIND SUSTAINED OR INCURRED IN CONNECTION WITH, OR RELATED TO, THE EQUIPMENT OR YOUR USE OF THE EQUIPMENT REGARDLESS OF THE FORM OF ACTION OR NATURE OF THE CLAIM (INCLUDING, BUT NOT LIMITED TO, BREACH OF WARRANTY, BREACH OF CONTRACT, TORT, NEGLIGENCE OR STRICT LIABILITY) AND WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE, AND EVEN IF WESTERN MULTIPLEX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS. IN NO CASE WILL WESTERN MULTIPLEX BE LIABLE FOR ANY REPRESENTATION OR WARRANTY MADE TO, OR BY, ANY THIRD PARTY BY, OR TO, YOU OR ANY OF YOUR AGENTS. WESTERN MULTIPLEX'S TOTAL LIABILITY TO YOU SHALL NOT EXCEED THE AMOUNT PAID BY YOU FOR THE EQUIPMENT AT ISSUE. This limitation of liability also applies to Western Multiplex's authorized resellers and distributors and it is the maximum amount for which Western Multiplex and the reseller or distributor who sold you the Equipment are collectively responsible.

## **6. DISCLAIMERS**

- 6.1 This Limited Warranty gives you specific legal rights, and you may also have other rights that vary from jurisdiction to jurisdiction. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, may not allow limitations on how long an implied warranty lasts, and may not allow provisions that permit a warranty to be voided. Consequently, such limitations and exclusions may not apply to you. In the event an implied warranty cannot be excluded under the law of the applicable jurisdiction, it is limited in duration to the applicable Warranty Period.

## **7. MISCELLANEOUS**

- 7.1 **Transfer.** You may not transfer or assign this Limited Warranty. Any transfers or assignments made in violation of this Paragraph shall be void.
- 7.2 **Governing Law.** The Limited Warranty shall be governed by the laws of the State of California, without reference to its conflicts of laws provisions. The United Nations Convention on the International Sale of Goods shall not apply to this Limited Warranty.
- 7.3 **Arbitration/Dispute Resolution.** Any dispute, controversy or claim arising out of or in connection with the Equipment shall be finally resolved by arbitration under the International Arbitration Rules of the American Arbitration Association. The place of arbitration shall be Sunnyvale, California. The number of arbitrators shall be one. The language of arbitration shall be English.
- 7.4 **Indemnification.** You shall indemnify and hold harmless Western Multiplex (including its directors, officers, employers and agents) against any and all claims (including all expenses and reasonable attorneys' fees) arising from or relating to the operation of the Equipment due to, in whole or in part, your (including your agents' or employees') negligence, gross negligence or misconduct.









# Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>1-1</b>
	PRODUCT HIGHLIGHTS .....	1-2
	KEY FEATURES.....	1-3
	HOW TO USE THIS MANUAL .....	1-3
	SAFETY INSTRUCTIONS .....	1-4
<b>2</b>	<b>SYSTEM OVERVIEW .....</b>	<b>2-1</b>
	POINT-TO-MULTIPOINT NETWORK MODEL.....	2-1
	Bridging and Address Filters .....	2-1
	Limitations of the Bridging Mode.....	2-2
	VLAN Switching – The PMP Implementation.....	2-3
	IP Routing and Default Gateway.....	2-5
	Address Filters in IP Routing Mode.....	2-6
	Proxy: to ARP or not to ARP.....	2-7
	Network Configurations in the IP Routing Mode.....	2-8
<b>3</b>	<b>SITE PLANNING &amp; INSTALLATION .....</b>	<b>3-1</b>
	General Considerations.....	3-1
	Weather.....	3-2
	Interference.....	3-3
	Antennas.....	3-4
	Path Planning.....	3-5
	SPECIFICATIONS .....	3-6
	SYSTEM.....	3-6
	STANDARDS COMPLIANCE AND INTERFACES.....	3-7
	CONFIGURATION AND MANAGEMENT.....	3-7
	POWER /ENVIRONMENT /SAFETY.....	3-7
	PHYSICAL DIMENSIONS.....	3-7
	INSTALLATION DETAILS.....	3-9
	Alternative Method of Connection.....	3-14
<b>4</b>	<b>SET-UP PROCEDURE.....</b>	<b>4-1</b>
	Important Configuration Notes .....	4-1
	Unpacking the System.....	4-2
	Mechanical Considerations – Mounting Units .....	4-3
	Pictures helpful for installation.....	4-5
	SOFTWARE INSTALLATION.....	4-7
<b>5</b>	<b>ADVANCED SETUP COMMANDS.....</b>	<b>5-1</b>
	BASE STATION CONFIGURATION COMMANDS.....	5-1
	Command to select frequency plan.....	5-1
	Command to assign the operating frequency.....	5-1
	Command to assign the first inbound slot.....	5-1
	Command to set the Base Station's Inbound Power Control margin, in dB.....	5-1
	Command to assign the number of reserved aloha channels.....	5-2
	Command to change the routing mode.....	5-2
	Command to turn the VLAN tagging on or off.....	5-2
	Command to display the Base Station's configuration settings.....	5-2
	Command to change the Base Station's IP address.....	5-2
	Command to change the Base Station's gateway IP address.....	5-2
	Command to change the Base Station's id.....	5-3
	Command to set the Base Station's subnet mask.....	5-3
	Command to activate range checking for all SUs associated with the Base Station.....	5-3
	Command to turn the Base Station's transmitter on or off.....	5-3
	Command to turn the Base Station's transmit power level.....	5-3
	Command to automatically turn on or off the transmitter upon power up.....	5-3

<i>Command to show the Base Station's arp table.....</i>	5-4
<i>Command to ping a device connected to the BSU .....</i>	5-4
<i>Command to turn data squelch on or off.....</i>	5-4
<i>Command to display the firmware version .....</i>	5-4
<i>Command to display available commands.....</i>	5-4
<i>Command to set frame synchronization mode .....</i>	5-4
SU CONFIGURATION COMMANDS .....	5-5
<i>Command to add a Subscriber Unit to the Base Station's database.....</i>	5-5
<i>Command to remove a Subscriber Unit from the Base Station database.....</i>	5-5
<i>Command to assign a VLAN ID to a Subscriber Unit.....</i>	5-5
<i>Command to assign a subnet mask to a Subscriber Unit.....</i>	5-5
<i>Command to set the SU's IP address.....</i>	5-5
<i>Command to display a Subscriber Unit's configuration parameters and traffic statistics .....</i>	5-5
<i>Command to display subscribe units that have entered the network.....</i>	5-5
<i>Command to add a static IP address of PC attached to a Subscriber Unit.....</i>	5-5
<i>Command to remove a static IP address from a Subscriber Unit.....</i>	5-6
<i>Command to disable a Subscriber Unit.....</i>	5-6
<i>Command to enable a Subscriber Unit.....</i>	5-6
<i>Command to set the gateway address of a Subscriber Unit.....</i>	5-6
<i>Command to set the IP Filter mode of a Subscriber Unit.....</i>	5-6
<b>6 TROUBLESHOOTING.....</b>	<b>6-1</b>
<i>Regular Maintenance .....</i>	6-1
<i>Problem – Solution .....</i>	6-1
<i>Unsolicited Base Station messages .....</i>	6-1
REPAIR AND RETURN INSTRUCTIONS AND POLICY STATEMENT.....	6-4
INDEX.....	6-5

## Figures

FIGURE 2-1: EACH HUB IS MADE UP OF ONE TO SIX BASE STATIONS AND MULTIPLE REMOTES(SUS) .....	2-1
FIGURE 2-2: MODEL OF THE PMP NETWORK .....	2-1
FIGURE 2-3: SU FILTERS IN BRIDGING MODE.....	2-2
FIGURE 2-4: FAN-OUT CAPABILITY OF A "TRUE" BRIDGING NETWORK .....	2-2
FIGURE 2-5: PMP VLAN IMPLEMENTATION .....	2-4
FIGURE 2-6: SU FILTERS IN IP ROUTING MODE .....	2-7
FIGURE 2-7: PROXY FOR REMOTE DEVICES RESIDING IN THE SAME SUBNET .....	2-8
FIGURE 2-8: EXAMPLE 1 NETWORK DIAGRAM .....	2-9
FIGURE 2-9: EXAMPLE 2 NETWORK DIAGRAM .....	2-10
FIGURE 3-1: CRIMPING STYLES AND INSERTION.....	3-10
FIGURE 3-2: INDOOR PORTION OF INTERCONNECT CABLE .....	3-11
FIGURE 3-3: IDU TO ODU CABLE .....	3-13
FIGURE 3-4: IDU TO ODU CABLE W/SEPARATE POWER PLUG.....	3-14
FIGURE 4-1: BASE UNIT KIT .....	4-2
FIGURE 4-2: BASE STATION UNIT ODU MOUNTING DETAIL.....	4-3
FIGURE 4-3: ODU WITH GPS ANTENNA.....	4-4
FIGURE 4-4: BASE STATION ODU .....	4-4
FIGURE 4-5: UP AND DOWN TILT LIMITS (-10 TO +5 DEGREES).....	4-5

## Tables

TABLE 2-1: PMP VLAN CONFIGURATION PARAMETERS FOR FIGURE 2-5 .....	2-4
TABLE 2-2: EXAMPLE 1 CONFIGURATION SETTING .....	2-8
TABLE 2-3: EXAMPLE 2 CONFIGURATION SETTING .....	2-10



# 1 Introduction

**T**sunami Multipoint is a point-to-multipoint outdoor wireless system offering a high-capacity alternative to wired data networks. Using IP packet radio transmitters, standard Ethernet interfaces, and an easy to-deploy design, the Tsunami Multipoint system enables high-speed network connections to multiple Ethernet switches, routers or PCs from a single location. With Tsunami Multipoint, you can now avoid the delays and costs associated with wired connections such as DSL, cable modems, and leased T1/E1 lines. Tsunami Multipoint eliminates wire/fiber installation costs and recurring monthly fees - delivering carrier-class performance at an affordable price.

Tsunami Multipoint systems consist of one or more Subscriber Units that communicate with a Base Station to provide high-performance wireless network connections.

## **EXTEND OR ENHANCE YOUR NETWORK OVERNIGHT**

With Tsunami Multipoint, there are no DSL, cable, or leased-line hassles to negotiate. You no longer have to worry about man-made barriers to overcome. Easy installation and operation allow network planners to quickly deploy up to 60 Mbps capacity between locations, making it the ideal solution for:

- Establishing high-speed connections between Internet Service Providers and their customers
- Organizations requiring high-capacity WAN connectivity between multiple buildings or campuses
- Organizations or service providers seeking network redundancy for mission critical wired connections

## **ABOUT THE TSUNAMI PRODUCT FAMILY**

The Tsunami family of Ethernet bridges provides wireless solutions that meet the growing demand for transparent and reliable high-speed network interconnectivity.

In addition to Tsunami Multipoint for point-to-multipoint connections, the Tsunami product line includes the following point-to-point offerings:

**Tsunami 10BaseT**, a cost-effective, high-capacity alternative to multiple wireline T1 connections.

**Tsunami 100BaseT/F**, a cost-effective, high-capacity alternative to wireline DS3 connections.

**Tsunami 1000BaseSX**, the world's first Ethernet bridge to provide gigabit, wireless connectivity for native IP connections.

## **PRODUCT HIGHLIGHTS**

### **UP TO 360 MBPS PER HUB SITE**

- Speeds of 20 Mbps Time Division Duplex (TDD) per Base Station for optimal network efficiency
- Configurable upstream/downstream bandwidth to optimize desired throughput
- Six Base Stations provide 360 degree coverage, delivering up to 360 Mbps per hub site

### **FAST AND EASY TO DEPLOY & MANAGE**

- Subscriber Unit simplicity enables self installation to minimize deployment costs
- Audible beeper alignment eases installation
- Subscriber Unit with integrated antenna connects to indoor power & networks using a single CAT5 cable
- "Over the air" software upgrades minimize subscriber unit maintenance costs

### **RAPID RETURN ON INVESTMENT**

- Rapid, easy deployment enables quick service activation, reduced costs and faster payback

## TSUNAMI POINT-TO-MULTIPOINT

- High-capacity connection enables faster network traffic to deliver new service offerings

### PURE ETHERNET CONNECTIVITY

- Operates in either Ethernet bridging or IP routing modes with direct connections to PCs, Fast Ethernet switches & routers
- Support for VLAN tagging

### KEY FEATURES


- Flexible throughput rates: Time Division Duplex (TDD)
- 5.8 GHz license-exempt frequency band
- Compliant with industry standards
- Base Station provides 60 degree antenna - six Base Stations cover 360 degrees
- Network management through SNMP & Java-based "Wireless Manager" software
- Point-to-multi point communications from less than 1 mile/kilometer to more than 5 miles/ 8 kilometers

---

#### ICON KEY


---

 Information

 Suggestion

 Caution

 Note

 Write this down

---

## How to Use This Manual

The “icon key” at left will be used to “highlight” specific text to call particular attention to it. Where specific emphasis needs to be placed, these icons will direct you to other information or particular areas where additional information can be found.



## Safety Instructions

### IMPORTANT

This product has been evaluated to the U.S. and Canadian (Bi-National) Standard for Safety of Information Technology Equipment, Including Electrical Business Equipment, CAN/CSA C22.2, No. 950-95 \* UL 1950, Third Edition, including revisions through revision date March 1, 1998, which are based on the Fourth Amendment to IEC 950, Second Edition. In addition, this product was also evaluated to the applicable requirements in UL 1950, Annex NAE.

WARNING - This unit is intended for installation in a Restricted Access location in accordance with Articles 110-18, 110- 26, and 110-27 of the United States National Electric Code ANSI/NFPA 70.

This equipment should be installed in accordance with Article 810 of the United States National Electrical Code.

When installed, this equipment is intended to be connected to a Lightning/Surge Protection Device that meets all applicable national Safety requirements.

Equipment is to be used and powered by the type of power source indicated on the marking label only.

This product is intended to be connected to an AC power source which must be electrically isolated from any ac sources and reliably earthed. Only an AC power source that complies with the requirements in the Standard for the Safety of Information Technology Equipment, Including Electrical Business Equipment, CAN/CSA C22.2, No. 950-95 \* UL 1950, Third Edition, can be used with this product. A 15-Amp circuit breaker is required at the power source. In addition, an easily accessible disconnect device should be incorporated into the facility wiring. Always use copper conductors only for all power connections.

WARNING - This equipment is intended to be earthed. Use only the power supply provided by Western Multiplex and be sure the ground pin is connected to an earthing conductor between the unit's earthing terminal and your earthing point.

Do not apply power to the equipment when the cable between the power source (Power Brick or Block) and the Out Door Unit is not yet connected properly.

Servicing of this product should be performed by trained personnel only. Do not disassemble this product. By opening or removing any covers you may expose yourself to hazardous energy parts. Incorrect re-assembly of this product can cause a malfunction, and/or electrical shock when the unit is subsequently used.

## **T S U N A M I M U L T I P O I N T**

Do not insert objects of any shape or size inside this product. Objects may contact hazardous energy parts that could result in a risk of fire or personal injury.

### **NOTE:**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### **CAUTION**

**The outdoor units of the Tsunami Multipoint products must be fixed mounted on permanent structures with a separation distance of at least 1.5 meters from all persons during normal operation.**

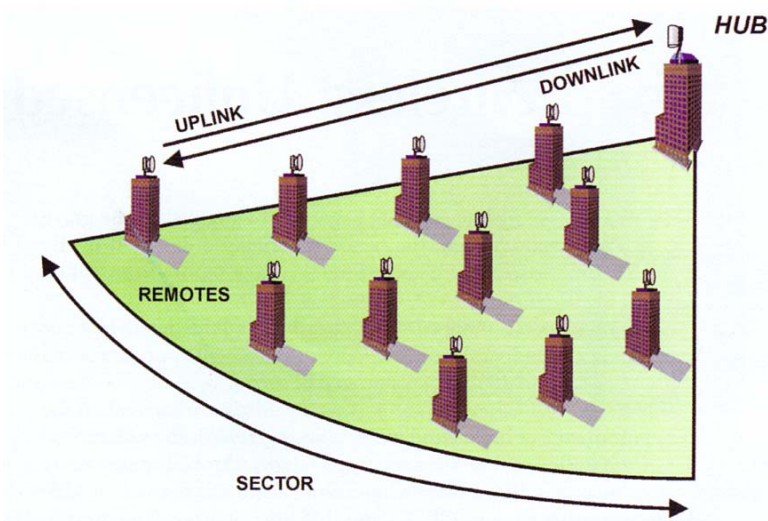
### **CAUTION:**

**Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment**



## 2 System Overview

A system is made up of one to six Base Stations that make up a Hub (or cell) with each Base Station communicating with their associated SUs (Subscriber Units). Together, they provide a wide coverage, high-capacity system that transfers IP traffic between the Hub and its multiple SUs. Each Hub has the ability to communicate in all directions using up to six sectors of 60 degrees each. Each of the Hub's six sectors has the capability of communicating 20 Mbps in total bandwidth allowing a maximum of 360 Mbps per Hub.



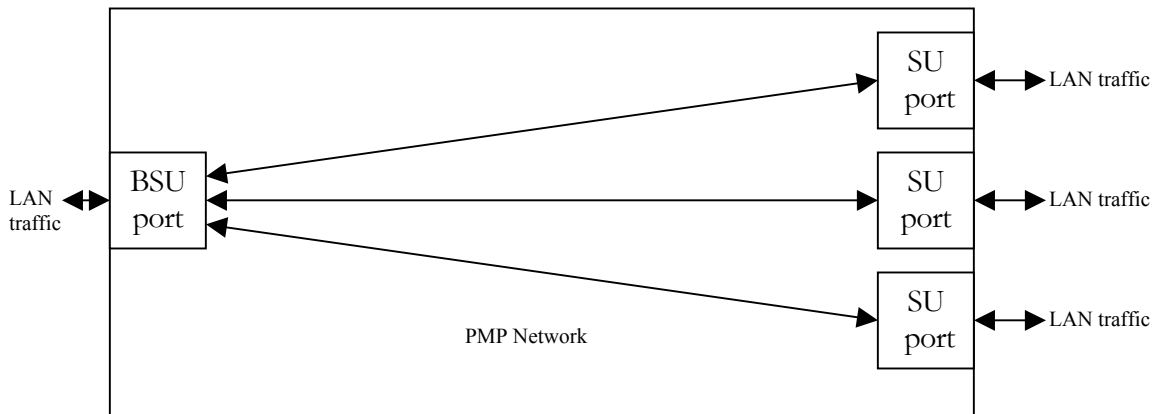
**Figure 2-1: Each HUB is made up of one to six Base Stations and multiple remotes(SUs)**

**Uplink and Downlink**, each SU communicates with a BSU in a coordinated manner so that all other remotes within the BSU's jurisdiction have an equal amount of time to coordinate their data needs in both the uplink and downlink sessions. All SUs are very quickly handled on a case by case basis giving the user, at the SU, the impression that they are in constant communication with its Hub's or BSU's Sector.



## Point-to-Multipoint Network Model

When we talk about the PMP network, one should look at the Subscriber Unit (SU) and the Base Station Unit (BSU) as an integrated transmission and switching medium with physical ports or access points that interface to end user devices. Each Base Station Unit or SU represents one such physical port or access point. Packets received by a SU are transmitted to the Base Station Unit and emerge out from it as a single data stream. Packets flowing into the Base Station Unit are broadcasted to the SUs, which select only packets destined for their local networks based on a set of filtering criteria.



**Figure 2-2: Model of the PMP network**

### Bridging and Address Filters

Depending on the transmission mode selected, the PMP network can function either as a "bridge" or as an "IP gateway" to the end user. In Bridging mode, the PMP network provides a direct physical connection between a SU and its Base Station Unit for the exchange of Ethernet frames between the two entities. To conserve wireless bandwidth, the SU uses some simple filtering criteria in hardware and software to prevent traffic destined for local network to be sent uplink. If the destination Ethernet address is not in the hardware table, the packet is given to software, which provides further filtering by matching the destination address with local addresses stored in its ARP table. The size of the ARP table is set to 512.

In the downlink direction, the outbound traffic is filtered in the SU via a "Programmable Hash Filter". If the destination Ethernet address of a downlink packet

triggers a "hit" in the hash list, the hardware will forward the packet to software for delivery to the local network. Otherwise, the packet is discarded.

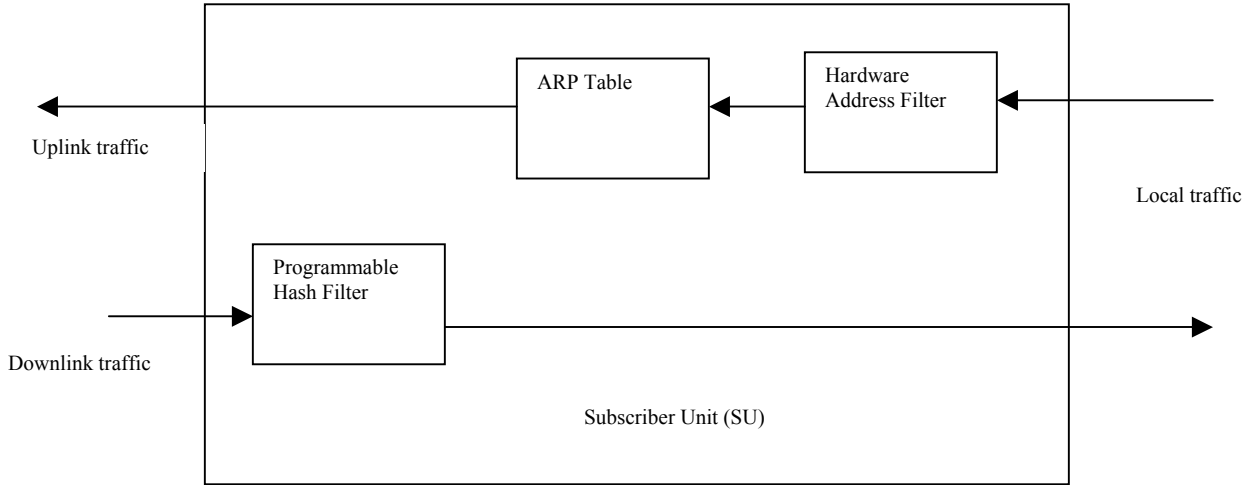


Figure 2-3: SU Filters in Bridging Mode

**Limitations of the Bridging Mode**

Again, if we consider the PMP network as a multi-port bridge, then it exhibits only a limited bridging function. For a true bridge to work, whatever traffic flows into one port should be fanned out to all the other ports, if the destination Ethernet address is not local to the receiving port. For the PMP network to behave the same, whatever data received by the Base Station Unit from a SU should also be broadcasted back downlink to all other SUs associated with the Base Station Unit. However, this is not done.

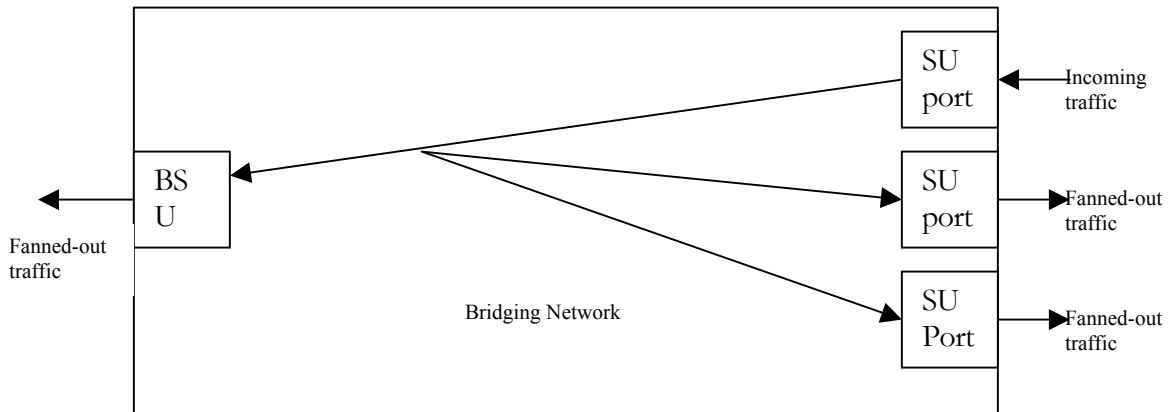


Figure 2-4: Fan-out capability of a "true" bridging network

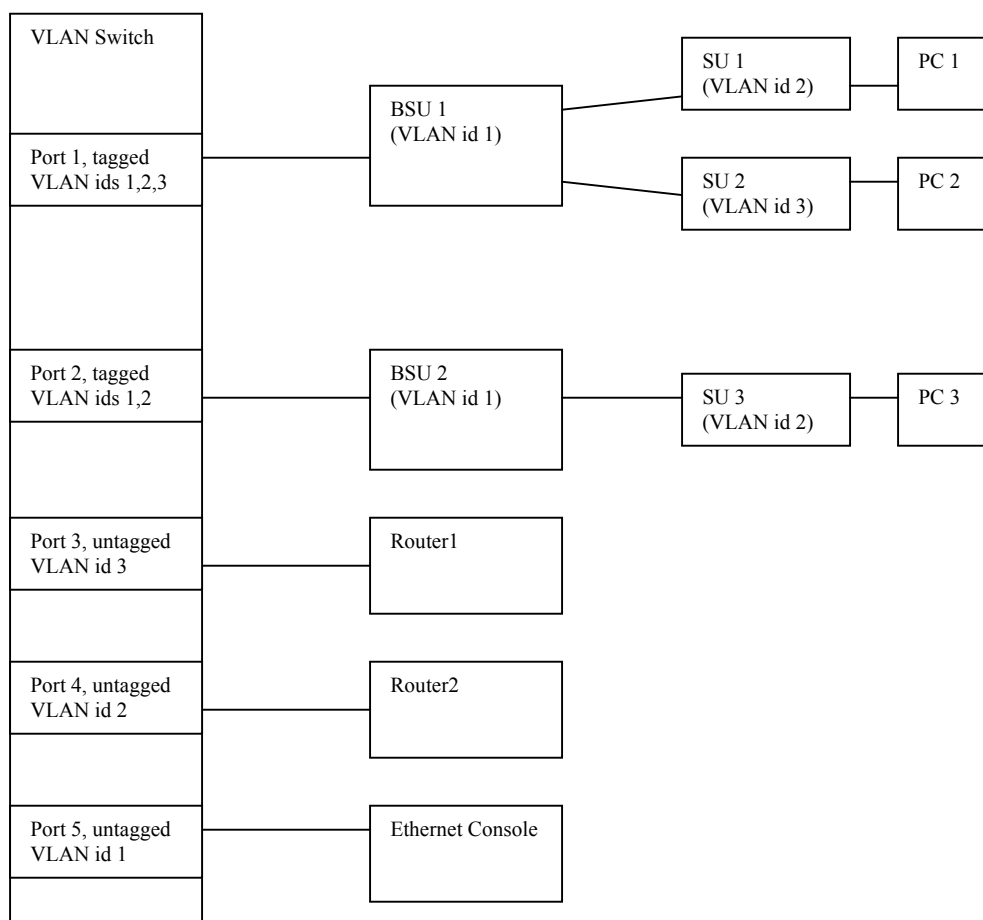
Other than the above constraint, Bridging mode also consumes more wireless bandwidth than IP Routing mode for several reasons. First, the entire Ethernet frame, which includes the 18 bytes Ethernet header, is transmitted between the SU and the Base Station Unit. Second, all ARP packets are transmitted between the SU and Base Station Unit as well. Empirical result has shown that in general Bridging mode can consume up to 10% more bandwidth than IP Routing mode.

### **VLAN Switching – The PMP Implementation**

VLAN switching is mainly used for segregating LAN traffic based on VLAN ID that accompanies a received VLAN frame. It allows a network operator to partition his LAN segment into closed user groups and allow a device to communicate only with other devices of the same group. Unlike a regular bridge, a VLAN switch is able to deliver received VLAN frames only to other ports tagged with the same VLAN ID, thus reducing unwanted network traffic.

VLAN switching is quick and simple from a switching node's perspective. However, setting up a VLAN network can be a mundane exercise for the network administrator. The reason is that most of the end user devices today (PCs for example) are not VLAN aware. This forces the network operator to place VLAN switches at critical junctions all over the place so that VLAN frames can be converted into regular Ethernet frames and vice versa. This can be a nightmare and a costly endeavor if proper planning does not take place beforehand. There is a built-in VLAN to Ethernet conversion capability in the SUs and Base Station Units, as illustrated in Figure 2-5.





**Figure 2-5: PMP VLAN implementation**

	VLAN TAG	VLAN ID	Routing Mode
BSU1	ON	1 (hard coded)	Bridging
BSU2	ON	1 (hard coded)	Bridging
SU1	Same as BSU1	2	Same as BSU1
SU2	Same as BSU1	3	Same as BSU1
SU3	Same as BSU2	2	Same as BSU2

**Table 2-1: PMP VLAN configuration parameters for Figure 2-5**

In Fig.2-5 above, the VLAN switch has both tagged and untagged ports. A tagged port can only receive and transmit VLAN frames. For a port such as port 1 that associates with multiple VLAN ids, it has to be tagged. An untagged port can receive both tagged VLAN frames or untagged regular Ethernet frames but will only transmit untagged Ethernet frames. An untagged port can only be associated with one unique VLAN id and is most commonly used for connection to VLAN unaware devices. As shown in Fig. 2.2, SU1, PC1, SU3, PC3 and router2 form a closed user group associated with VLAN id 2. SU 2, PC2 and Router1 form another closed user group associated with VLAN id 3. When SU1, for example, receives a regular Ethernet frame from PC1, it tagged the frame with VLAN id 2, which is SU1's configured VLAN id. The VLAN frame is passed to the VLAN switch via BS1 and broadcasted to port 2 and port 4 of the VLAN switch. When SU3 receives the VLAN frame from BS2, it converts the VLAN into regular Ethernet frame and gives it to PC3.

For control purpose, the VLAN IDs of all Base Station Units are hard coded to 1 and cannot be changed by the operator. For any device such as Wireless Manager or Ethernet Console to communicate with a Base Station Unit, the device needs to be connected to an untagged VLAN port associated with VLAN ID 1. Otherwise, the Base Station Unit will not be reachable. When a Base Station Unit wants to transmit a control message or send a response back to the Wireless Manager or Ethernet Console, it will transmit a tagged VLAN frame of id 1, which will be received by all devices connected to VLAN ports associated with VLAN id 1.

In PMP network VLAN switching is a special Bridging mode with the VLAN tag enabled in the Base Station Unit configuration. As such, VLAN switching is also bounded by the same constraint that SUs within the same Base Station Unit cannot communicate with each other. VLAN switching is not supported in IP routing mode.

## **IP Routing and Default Gateway**

In IP routing mode, a SU performs the following functions. First, it serves as a DHCP relay agent that facilitates the exchange of DHCP packets between the local PC and a remote DHCP server and also automatically becomes the PC's default IP gateway at the end of the process once the PC obtains its IP address assignment. Second, the SU provides additional network security measures by blocking any unauthorized PCs from accessing the wireless network. Four access modes have been implemented, as described below:

### **A: RESTRICTED ACCESS**

In this mode, for any device with an IP address not obtained from DHCP to access the PMP network, its static IP address must first be recorded in the PMP's database. We allow up to 5 static IP addresses to be associated with each SU.

In the Restricted mode, the Programmable Hash Filter discussed earlier contains only the DHCP based IP addresses, the static IP addresses and the gateway address that

have been registered. Any device with an IP address not in the PMP's configuration database will not be able to access the wireless network.

#### **B. LOCAL ACCESS**

In this mode, any device connected directly to the SU's local network will be able to access the network, regardless of how its IP address is obtained.

#### **C. OPEN ACCESS**

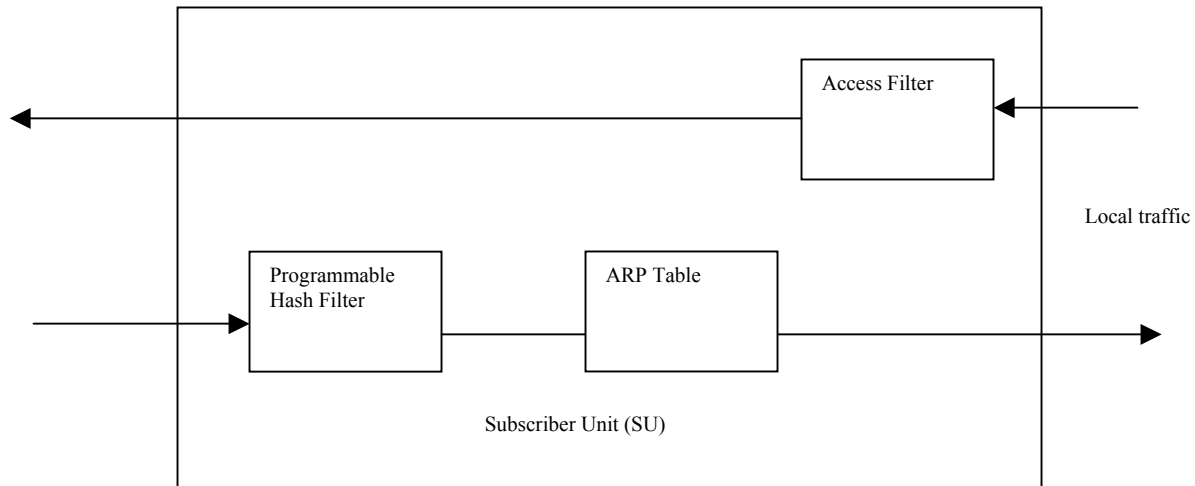
This mode allows any device connected either directly to the SU's local network or indirectly via a router to access the wireless network. When this mode is activated, the Programmable Hash Filter is disabled, allowing the SU software to receive all downlink packets. If the downlink packet is destined for the SU's local network, the software will deliver the packet directly. If the downlink packet belongs to a different subnet or network, the software will forward the packet to its gateway, which serves as the SU's default gateway to external networks.

#### **D. SUBNET ACCESS**

This mode is same as the Local Access Mode except that the Programmable Hash Filter is opened wide enough just to include all IP addresses that reside within the SU's own subnet.

### **Address Filters in IP Routing Mode**

In IP Routing mode, the uplink filtering is done via the access control mechanisms as described earlier. For downlink direction, IP addresses instead of Ethernet addresses are used in the hash filter. If a hash hit is triggered, the software will search its ARP table to locate the destination Ethernet address that corresponds to the destination IP address contained in the packet. If an entry is not found the packet will be discarded.



**Figure 2-6: SU Filters in IP Routing Mode**

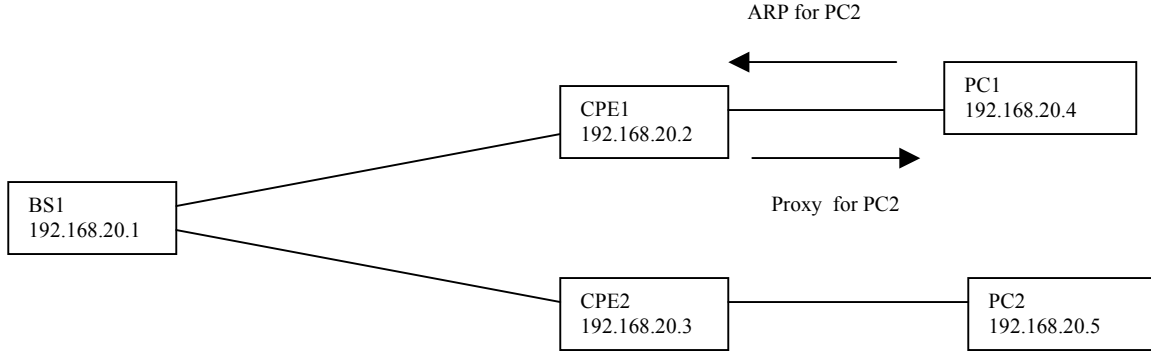
### Proxy: to ARP or not to ARP ...

In addition to enforcement of the access modes discussed above, one of the main functions of the SU is to serve as a proxy server for the local devices. Without this function many of our network applications will fail. Before we go into detailed discussions, however, we need to first understand the basics in IP networking.

When a device such as a PC, router, SU or Base Station Unit wants to transmit an IP packet, it needs to first decide if the destination IP address resides within its own subnet. If the answer is yes, the sending device needs to search for the corresponding Ethernet address associated with the destination IP address by broadcasting an ARP request to its local network. A device with a matching IP address or one which is interested in receiving packets for that IP address will send back an ARP response, which contains the destination Ethernet address. Once the destination Ethernet address is known, the sending device can then deliver the packet directly to that Ethernet address. If the destination IP address resides in a different subnet, then the sending device will not even bother to issue an ARP request but will instead forward the packet to a default gateway for delivery.

Now back to the PMP discussion. In the PMP network, it is quite common to have multiple SUs share the same subnet address. In that case, when a PC connected to a SU wants to send packets to a PC connected to another SU, the originating PC will issue an ARP request to explore the Ethernet address of the destination PC, since both of them reside in the same subnet. Unfortunately, the destination PC will not be able to receive the ARP request because it is not physically connected to the originating PC. This then forces the SU connected to the originating PC to issue a proxy response on behalf of the destination PC. The SU will issue a proxy response only when it knows via initial learning that the destination PC is not connected to its local network.

The proxy capability allows SUs in the PMP network to share the same subnet address, even though they are not directly connected. Without this capability, all the SUs in the network will be forced to have different subnet addresses.



**Figure 2-7: Proxy for remote devices residing in the same subnet**

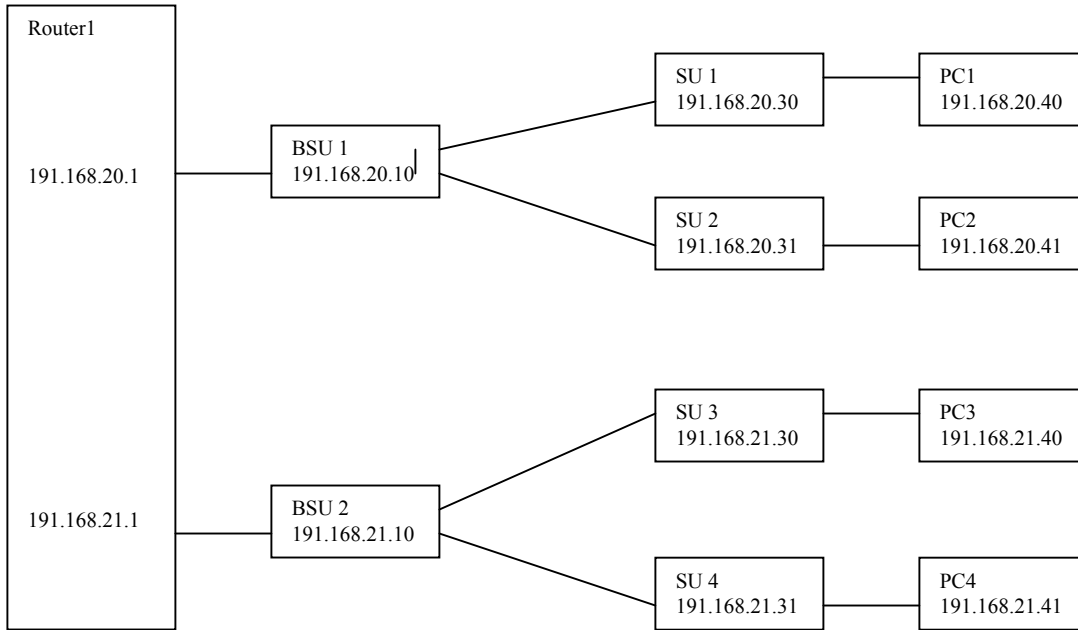
### Network Configurations in the IP Routing Mode

In the PMP network, IP routing mode is superior to Bridging mode for several reasons. First, as mentioned earlier, IP Routing mode conserves wireless bandwidth. Second, it provides added control over which hosts attach to the network. Third, it allows communications among end user devices associated with the same Base Station Unit. Fourth, it gives the network operator greater freedom in partitioning his network into logical subnets. However, if the operator expects his network to run smoothly in IP Routing mode, some careful forward planning will be required, as illustrated in the following examples.

#### Example 1

	Hash Mode	Static IP Address	DHCP IP Address	Subnet Mask	Default Gateway
Router1	NA	NA	NA	255.255.255.0	BSU1 for 192.168.20.0 subnet BSU2 for 192.168.21.0 subnet
BSU1	NA	NA		255.255.255.0	Router1
BSU2	NA	NA		255.255.255.0	Router1
SU1	Restricted	PC1	NONE	255.255.255.0	NONE
SU2	Restricted	PC2	NONE	255.255.255.0	NONE
SU3	Restricted	NONE	PC3	255.255.255.0	NONE
SU4	Restricted	NONE	NONE	255.255.255.0	NONE
PC1	NA	191.168.20.40	NONE	255.255.255.0	SU1 (via configuration)
PC2	NA	191.168.20.41	NONE	255.255.255.0	SU2 (via configuration)
PC3	NA	NONE	191.168.21.40	255.255.255.0	SU3 (via DHCP)
PC4	NA	NONE	191.168.21.41	255.255.255.0	SU4 (via DHCP)

**Table 2-2: Example 1 configuration setting**



**Figure 2-8: Example 1 Network Diagram**

In this configuration two subnets 191.168.20.0 and 191.168.21.0 are installed. BS1 belongs to subnet 191.168.20.0 and is connected to one of the router ports, which has the same subnet address. BS2 belongs to subnet 192.168.21.0 and is connected to a second router port with the same subnet address.

For PC1 to send a packet to PC2, it will first issue an ARP request, which SU1 will respond on behalf of PC2 as part of the proxy process described earlier.

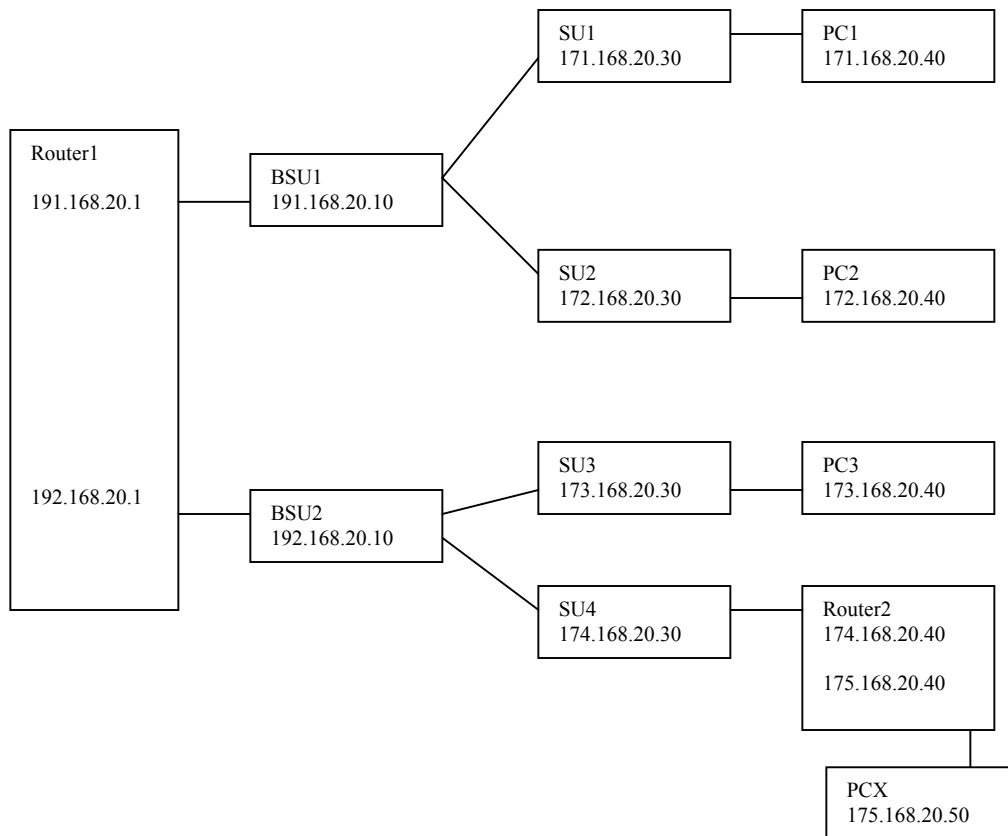
PC1 then transmits data packets to SU1, which forwards only the IP portion to BS1 after stripping off the 18 bytes Ethernet header. BS1 delivers the packet to Router1 after appending its own Ethernet address as the source Ethernet address. Router1 recognizes that the destination address belongs to subnet 192,168,20,0 and forwards it back to BS1 via the same router port. The packet is received by SU2 via BS1 and filtered via the Programmable Hash Filter since PC2's address is already recorded in SU2's database. The packet is delivered to software, which searches via its ARP table, appends PC2's Ethernet address as the destination Ethernet address and its own address as the source Ethernet address and delivers the packet to PC2.

For PC1 to send a packet to PC3, it will forward the packet to SU1 since the destination address lies outside of PC1's subnet and also that SU1 is PC1's default gateway. When Router1 receives the packet it recognizes that the destination address belongs to a different subnet than that of the receiving port. The packet is then sent to BS2 via the other router port and is ultimately received by PC3 following similar process described above. PC4 cannot access the network because its IP address is not recognized by the SU in Restricted mode.

**Example 2:**

	Hash Mode	Static assigned IP Address	DHCP assigned IP Address	Subnet Mask	Default Gateway
Router1	NA	NA	NA	255.255.255.0	BS1 for 171.168.20.0 and 172.168.20.0 subnets BS2 for 173.168.20.0, 174.168.20.0 and 175.168.20.0 subnets
Router2	NA	NA	NA	255.255.255.0	SU4 for 174.168.20.0 subnet
BS1	NA	NA	NA	255.255.255.0	Router1
BS2	NA	NA	NA	255.255.255.0	Router2
SU1	Restricted	PC1	NONE	255.255.255.0	NONE
SU2	Restricted	PC2	NONE	255.255.255.0	NONE
SU3	Restricted	NONE	PC3	255.255.255.0	NONE
SU4	Open	NONE	NONE	255.255.255.0	Router2
PC1	NA	171.168.20.40	NONE	255.255.255.0	SU1
PC2	NA	172.168.20.40	NONE	255.255.255.0	SU2
PC3	NA	NA	173.168.20.40	255.255.255.0	SU3
PCX	NA	NA	175.168.20.40	255.255.255.0	Router2

**Table 2-3: Example 2 Configuration Setting**



**Figure 2-9: Example 2 Network Diagram**

For illustrative purpose, all SUs and Base Station Units are assigned to different networks. This is possible because in IP Routing mode the PMP network can function like a multi-port router where each port has its own network address. In this configuration we have added Router2, which is connected to SU4 and also to PCX via a second port with a different network interface 175.168.20.0. In order for SU4 to receive IP packets for PCX or any unknown device that is connected to Router2, its hash mode must be set to OPEN. For PCX to send data to PC2, it will deliver the packet to Router2, which is PCX's gateway to the PMP network. Router2 forwards the packet to SU4, which is its default gateway. SU4 delivers the packet to Router1 via BS2. Router1 forwards the packet to BS1. The packet is received by SU2 and delivered to PC2. If PC2 wants to send packet to PCX, it will forward the packet to SU2, which delivers the packet to Router1 via BS1. Router1 then sends the packet to SU4 via BS2. Since hash mode for SU4 is set to OPEN, the hardware will deliver the packet to software bypassing the Programmable Hash Table. SU4 recognizes that this packet is for a different subnet and forwards it to Router2 for delivery to PCX.

#### **USEFUL HINTS FOR TESTING PMP NETWORK UNDER BRIDGING MODE**

Before changing the Base Station Unit Configuration to VLAN switching, make sure that the Base Station Unit and the Ethernet console are connected to a VLAN switch. Otherwise, you will not be able to talk to the Base Station Unit again since the PC hosting the Ethernet Console cannot send or receive VLAN frames.

#### **USEFUL HINTS FOR TESTING PMP NETWORK UNDER IP ROUTING MODE**

Make sure to configure the Base Station Unit to have the router port as its default gateway and that the IP addresses of the Base Station Unit and the router port reside in the same subnet. Also remember to configure the router port to point to the Base Station Unit as its gateway.

Make sure that a SU and its directly connected devices are in the same subnet. The subnet address of a device can be obtained by logically "AND" the device's IP address with its subnet mask. A subnet mask of 255.255.255.0 implies that there are 255 IP addresses within the same subnet.

If the IP address of a PC connected to a SU is not dynamically assigned, make sure that the PC's IP address appears in the SU's static IP list. Otherwise, the PC will not be able to access the wireless network if the SU is running in Restricted mode. Also, remember to configure the PC to point to the SU as its default gateway.

In the latest firmware release, the proxy setting is turned on automatically – don't change the setting.



**USEFUL HINTS FOR ANYONE TRYING TO OPERATE THE PMP NETWORK**

When changing back and forth between Bridging mode and IP routing mode, always remember to manually clear the ARP table of your PC.

Don't just turn off the power of the Base Station Unit "at-will" because the Base Station Unit might be saving internal variables or configuration parameters to the flash memory at that moment. Always wait for a minute after keying in an operator command before shutting the Base Station Unit down.

It is wise to connect a Wireless Manager (WM) to the PMP network. The WM serves as an external data storage and configuration backup for the PMP network, even if we don't care about its other features. The configuration is downloaded from WM to a Base Station Unit every time the Base Station Unit is powered up.

Always follow the simple proxy rule and fundamental principles concerning subnet and default gateway in planning and analyzing the PMP network. A good understanding of the basic IP Networking is needed regardless of whether you operate the PMP network in IP Routing or Bridging mode.

If you cannot get the network to work - most likely there is a set up error. Check the network configuration using the above hints and try again.

## 3 Site Planning & Installation

The installation of a wireless network requires much the same basic planning as any wired network. The main difference is that the wireless signal requires some additional planning. This planning includes RF path planning, site preparation, and installation of outdoor components such as outdoor units, antennas, lightning protection devices, and cabling suitable for outdoor conditions.

Although the technology implemented in this broadband fixed wireless system can make use of multipath signals, reducing the effect of obstructions in the path, it is important that the characteristics of the path be carefully examined. With this knowledge, components and network requirements can be correctly planned for your specific application.

This chapter provides insight into the planning necessary to prepare your site for your broadband fixed wireless system.

### General Considerations

A basic consideration is the physical location of the sites at each end of the link. Because microwave signals travel in a straight line, a clear line of sight between antennas is ideal. Frequently, however, the locations of the desired links are fixed. When a clear line of sight cannot be achieved, you must plan accordingly.

Other general site considerations include:

- a. Will a tower have to be constructed? Are permits required?
- b. Possibility of future obstructions-Will trees grow high enough to interfere with the signal? Are there plans to erect buildings between the sites that may obstruct the path?
- c. Availability of grounding-Good grounding is important in all areas of the world, but in areas prone to lightning, it is especially critical.
- d. Distance between the indoor portion of the system and the user's network.
- e. The SU may potentially be served by different Base Stations. Can the best BSU access and available sighting location be determined prior to installation.

The planning of a wireless link involves collecting information and making decisions. The following sections will help you determine which information is critical to the site and will be an aid in the decision-making process.

## **Weather**

It is important to research any unusual weather conditions that are common to the site location. These conditions can include excessive amounts of rain, wind velocity or extreme temperature ranges. If extreme conditions exist that may affect the integrity of the radio link, it is recommended that these conditions be taken into consideration early in the planning process.

### **RAIN**

Except in extreme conditions, attenuation (weakening of the signal) due to rain does not require serious consideration for frequencies up to the range of 6 GHz. When microwave frequencies are at 10-12 GHz range or above, attenuation due to rain becomes much more of a concern, especially in areas where rainfall is of high density and long duration. The systems discussed in this manual operate at frequencies below 6 GHz, so rain is not a concern.

Temperature can adversely affect the radio link when such as temperature inversion, or very still air accompanied by stratification. Temperature inversion can negate clearances, and still air along with stratification can cause severe refractive or reflective conditions, with unpredictable results. Temperature inversions and stratification can also cause ducting, which may increase the potential for interference between systems that do not normally interfere with each other. Where these conditions exist, it is recommended that shorter paths and adequate clearances are used.

### **WIND**

Any system components mounted outdoors will be subject to the effect of wind. It is important to know the direction and velocity of the wind common to the site. Antennas and their supporting structures must be able to prevent these forces from affecting the antenna or causing damage to the building or tower on which the components are mounted. Antenna designs react differently to wind forces, depending on the area presented to the wind. This is known as wind loading.

Note For definitions of wind loading specifications for antennas and towers, refer to TIA/EIA-195 (for antennas) or TIA/EIA-222 (for towers) specifications.

### **LIGHTNING**

The potential for lightning damage to radio equipment should always be considered when planning a wireless link. A variety of lightning protection and grounding devices

are available for use on buildings, towers, antennas, cables, and equipment, whether located inside or outside the site, that could be damaged by a lightning strike.

Lightning protection requirements are based on the exposure at the site, the cost of link down-time, and local building and electrical codes. If the link is critical, and the site is in an active lightning area, attention to thorough lightning protection and grounding is critical.

### **LIGHTNING PROTECTION**

To provide effective lightning protection, install antennas in locations that are unlikely to receive direct lightning strikes, or install lightning rods to protect antennas from direct strikes. Make sure that cables and equipment are properly grounded to provide low-impedance paths for lightning currents. Install surge suppressors on adjacent telephone lines and power lines.

Recommended is additional lightning protection in those regions that have extreme lightning occurrences for cables leading to the wireless OutDoor Unit (ODU) to/from the indoor power brick. This optional lightning protection should be placed at points close to where the cable passes through the bulkhead into the building, as well as near the ODU. Use the earthing screw at the ODU and use proper grounding.

### **CAT5 CABLE**

When the entire control cable, from the building entrance to the ODU, is encased in steel conduit, no surge arrestors are required. Otherwise, each control cable requires one surge arrestor within two feet of the building entrance.

**Note** For installations with several radios, it may be more convenient to use a Type-66 punch block with surge arrestors. A Type-66 punch block can accommodate up to 25 conductor pairs.

## **Interference**

An important part of planning your broadband fixed wireless system is the avoidance of interference. Interference can be caused by effects within the system or outside the system. Good planning for frequencies and antennas can overcome most interference challenges.

### **CO-CHANNEL AND ADJACENT CHANNEL INTERFERENCE**

Co-channel interference results when another RF link is using the same channel frequency. Adjacent-channel interference results when another RF link is using an adjacent channel frequency. In selecting a site, a spectrum analyzer can be used to determine if any strong signals are present at the site and, if they are, to determine how

close they are to the desired frequency. The further away from your proposed frequency, the less likely they are to cause a problem.

**Antennas**

Antennas frequently play a key role in reducing the potential for interference. They come in a variety of configurations that have different performance characteristics in the areas of gain and directionality. Antennas that transmit/receive in all directions are known as omni-directional, while those that transmit/receive in one specific direction are categorized as directional. Antennas also vary in beamwidth, which is the aperture to which they can “see” signals. Larger antennas typically provide narrower beamwidths and can diminish interference from nearby transmitters by:

- Focusing RF energy from the intended destination
- Reducing the power of interfering sources not directly aligned to the antenna

Antennas: the narrower, the better

Tsunami Multipoint Ethernet Systems use integrated directional antennas that transmit and receive a relatively narrow beamwidth of radio energy, improving system performance by reducing the likelihood that surrounding RF clutter will interfere with reception. The antennas with this system are directional and can not be detached.

Type:	Flat-panel antenna
Beamwidth:	60-degree
Elevation:	6-degree

Even when other licensees are not an issue, if you are using a network deployment using the "cell" approach, all these considerations are still important to reduce interference between your own adjacent installations. Antennas are tuned to operate on a specific group of frequencies. Tsunami Multipoint offers a variety of channel plans that provide a flexible tool for overcoming present and future interference. Four non-overlapping 20 MHz channels (six total directional channels) can be used to avoid existing traffic in the 5.8 GHz frequency band. If one part of the 5.8 GHz spectrum is occupied when Tsunami Multipoint is initially deployed, another frequency channel can be selected to bypass the interfering signal. If interference arises after deployment, another frequency channel plan can be selected to “steer around” the impacted channel. Beamwidth and gain have been optimized in this equipment.

**ANTENNA POLARIZATION**

The Tsunami Multipoint system uses left-hand circular polarization. As a result, the signal is successfully received regardless of the orientation of the antenna. Circular

polarization also provides protection against multipath degradation of the signal quality.

### **TOWERS**

When planning antenna placement, it might be necessary to build a free-standing tower for the antenna. Regulations and limitations define the height and location of these towers with respect to airports, runways, and airplane approach paths. These regulations are controlled by the FAA. In some circumstances, the tower installations must be approved by the FAA, registered with the FCC, or both.

To ensure compliance, review the current FCC regulations regarding antenna structures. These regulations (along with examples) are on the FCC web site at [www.fcc.gov/wtb/antenna/](http://www.fcc.gov/wtb/antenna/).

### **Path Planning**

To get the most value from a wireless system, path planning is essential. In addition to the fact that radio signals dissipate as they travel, many other factors operate on a microwave signal as it moves through space. All of these must be taken into account, because any obstructions in the path will attenuate the signal.

### **CALCULATING A LINK BUDGET**

A link budget is a rough calculation of all known elements of the link to determine if the signal will have the proper strength when it reaches the other end of the link. To make this calculation, the following information should be considered.

A signal degrades as it moves through space. The longer the path, the more loss it experiences. This free-space path loss is a factor in calculating the link viability. Free-space path loss is easily calculated for miles or kilometers.

Availability represents the quality of a link. It is the ratio of the time that the link is available to the total time. This serves as a guide to the service that you can expect, on average, over a period of one year. Table 2-2 shows how percentage availability relates to outage time per year.

Note: use the path planning tools located on the WMUX web site: [www.wmux.com](http://www.wmux.com)

Note You can lower the bit error rate (BER), resulting in greater reliability, by reducing the data throughput or reducing the distance.

### **UNLICENSED FREQUENCIES-ISM**

The FCC has identified the frequencies from 5.725 to 5.825 GHz as an Industrial, Scientific, Medical (ISM) band. This band can be used by anyone without having to

obtain a license. However, you must use radio equipment that is "type approved" by the FCC or local government for use within the specific band.

## Specifications

PRODUCT	BURST-RATE LIMIT	MODEL NUMBER
Base Station Unit	20 Mbps	40400-25x

BURST RATE	D/L THROUGHPUT	U/L THROUGHPUT
20 Mbps	9 Mbps	8 Mbps

Note: Above calculations are typical and based on a 50/50 down/link (D/L) up/link (U/L) division of slots. SU throughput may be limited by a provider's Service Level Agreement or other D/L U/L settings

TX POWER	+6 to +17 dBm (into antenna port)
----------	-----------------------------------

ANTENNA	Integrated, LHCP 19dBi
---------	------------------------

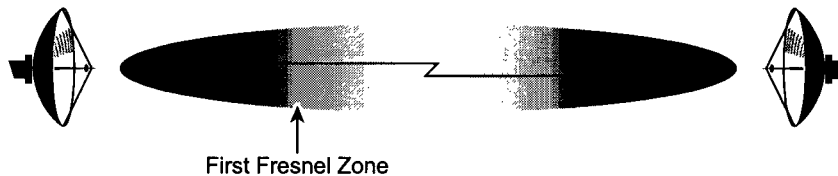
RECEIVER SENSITIVITY	BURST-RATE	THRESHOLD
	20 Mbps	-89 dBm

### MAXIMUM DISTANCE TO SUBSCRIBER UNIT

BURST-RATE	CLOS*	NLOS**
20 Mbps	6 miles/10 km	3 miles/5 km

\* *Clear-Line-of-Site distance is calculated for 99.995% availability assuming no obstructions in the first Fresnel zone.*

\*\* *Near-Line-of-Site distance is for a typical installation with moderate multipath/shadowing due to terrain and structures.*



## SYSTEM

Operating Frequency Range	5725-5825 MHz
---------------------------	---------------

Radio Access Method	TDMA
Duplexing	Time Division Duplex (TDD)
Integrated Antenna	19 dBi (60° Azimuth. x 6° Elevation)
Max Subscriber Units/BSU	1,023
Frequency Channels	4 non-overlapping, 5 and 6 available
Regulatory Compliance	FCC Part 15.247 (ISM) IC RSS210

**STANDARDS COMPLIANCE AND INTERFACES**

Ethernet Interface	10/100BaseT
Ethernet Connector	RJ45 female
BSU indoor-outdoor cable	Circular plastic connectors with Category-5 cable
Standards Compliance	IEEE 802.1d Bridging Mode IEEE 802.1q VLAN

**CONFIGURATION AND MANAGEMENT**

Configuration	via Ethernet or Wireless Manager
SNMP Agent	MIB II ( <i>future release</i> )
Security	Authentication, IP/MAC Filtering
Software Upgrades	Over-the-air Subscriber Unit reprogramming Downloadable Base Station reprogramming

**POWER /ENVIRONMENT /SAFETY**

Electrical	
Base Station Unit	-36 to -60 Volts DC, 1.25 Amps
Base Station Unit Power Brick	100-240 Volts AC
Base Station Unit Power Block	-48 Volts DC
Operational Temperature	0° to 55° C (indoor), -33° to 65° C (outdoor)
Humidity	95% non-condensing (indoor) 5% to 100%, condensing (outdoor)
EIVIC	FCC Class B
Safety	UL-1950
Environmental Compliance	ETS 300 019

**PHYSICAL DIMENSIONS**

Base Station (Outdoor Unit)	
Size (WxHxD)	10.2 x 24 x 6.6 inches/25.9 x 61 x 16.8cm
Weight	20 lbs/9 kg
Base Station Power Block (Indoor Unit, for up to 6 Base Stations)	



Size (WxHxD)	17.2 x 3.5 x 8.25 inches/43.7x8.9x 21cm
Weight	5 lbs/2.3 kg
Base Station Power Brick (Indoor Unit, for 1 Base Station)	
Size (WxHxD)	37.4x 70.9 x 24.8 inch/95 x 180 x 63 cm
Weight	1.5 lbs/0.7 kg

# INSTALLATION Details

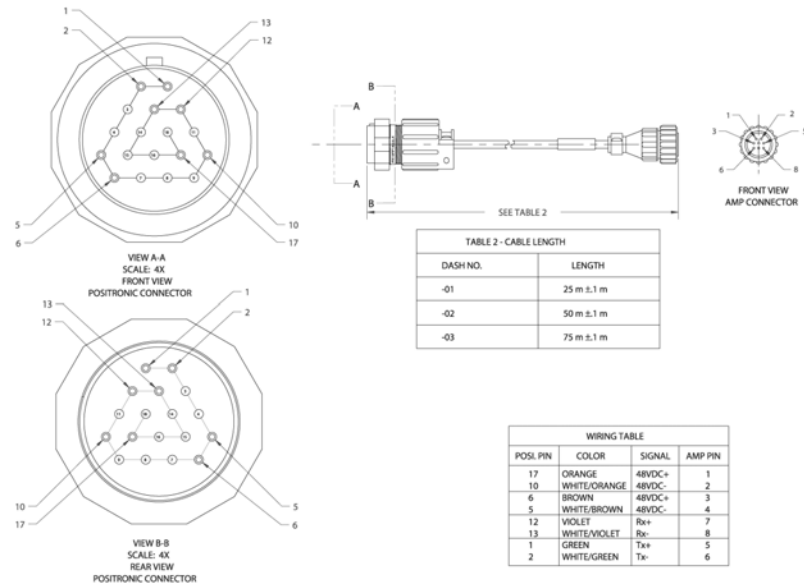
Base Station Unit (ODU)

Pole Mounting, 1.5-3.00" diameter

## OPTIONAL ACCESSORIES

Connector kit

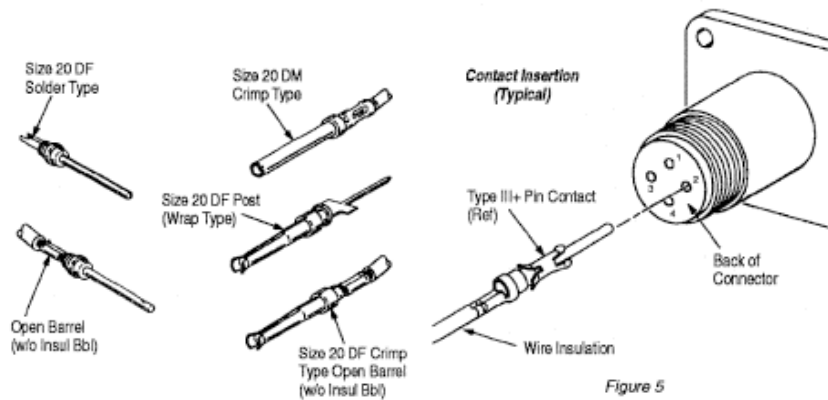
Other cable lengths (25 & 50m cables)



**Figure 3-1: BSU's ODU Cable Detail**

## Crimping Method for Connector Termination

Loose piece contacts are designed to be crimped with crimp tooling (hand tools, die assemblies, or crimping heads), but can be done with normal hand tools. The applicable crimp tooling for the contacts is described later. Read the material packaged with the crimp tooling for the proper crimping procedure.



**Figure 3-2: Crimping styles and insertion**

**Insertion** - Normally, an insertion tool is not required to insert contacts into the housings. However, if the wire bundle is large, or if the wire is fragile, an insertion tool is recommended.

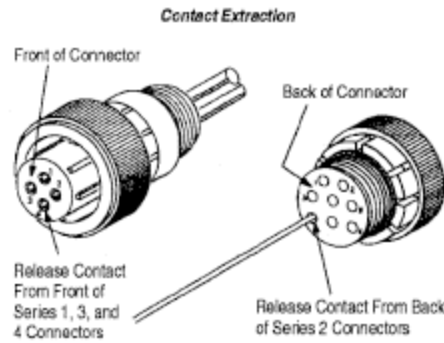
To insert a contact, grip insulation of wire (directly behind contact) and align contact with BACK of desired contact cavity. Insert contact straight into cavity until it bottoms. Pull back lightly on wire to be sure contact is locked in place.

**Extraction** - Extraction tools are designed for removing pin and socket contacts from the connectors. Refer to the instruction material packaged with the tool for the proper extraction procedure.

### MATING CONNECTORS

These connectors have a positive lock feature which prevents accidental disengagement. Align polarizing keys and keyways and start plug into receptacle. Rotate coupling ring CLOCKWISE until positive lock snaps into position.

*Do not use* for blind mating applications.



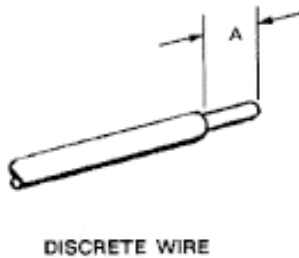
**Figure 3-3: Indoor portion of interconnect cable**

### Wire Size and Preparation

Contacts are available for the wire sizes specified. Prepare wire for crimping by stripping insulation. DO NOT nick, scrape, or cut the stranded or solid wire conductor during stripping operation.

*When using twisted pair cable, one wire should be cut shorter than the other by the same distance as the strip length of the longer wire.*

### Wire Preparation



### Loading Contact Into Housing

Normally an insertion tool is not required to insert contacts into housings. However, if the wire bundle is large or the individual wires are fragile, the use of an Insertion tool is recommended.

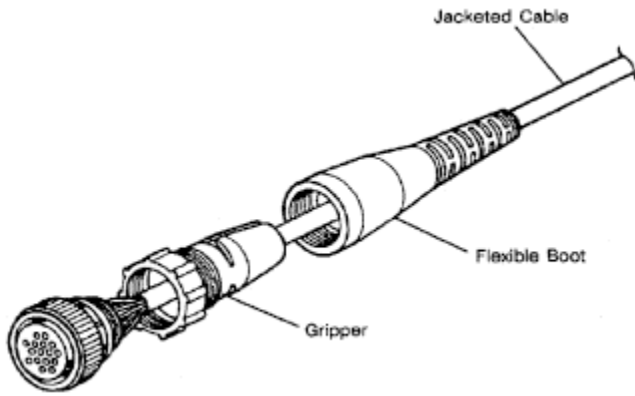
### Shield and Strain Relief

If wire at the rear of the housing is subjected to strain, use of a strain relief will prevent damage to the contacts, wires, and housing.

#### Strain Relief Kits

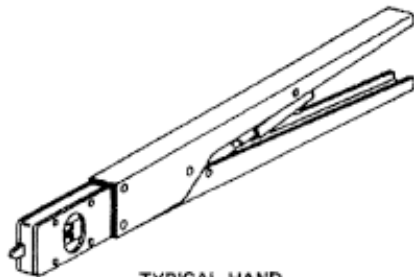
Several types and sizes of strain relief kits are available. Shield and strain relief kits include a shield, strain relief clamps, and two self-tapping screws. Flexible strain relief boots and grippers are used with jacketed cable (or firmly taped discrete wires) to provide wire protection and prevent contact pullout when severe cable angle applications are encountered, or when connectors are frequently disconnected and reconnected. Heat shrink sealing boots can also provide a splash-proof strain relief for jacketed cable.

*NOTE If a strain relief is used on the connector, the wires may be dressed to an angle at the end of the strain relief. However, without use of a strain relief, the wires should not be dressed closer than 2.50 inches from the back of the housing. To prevent damage to contacts and/or housing, avoid exerting stress on wire.*

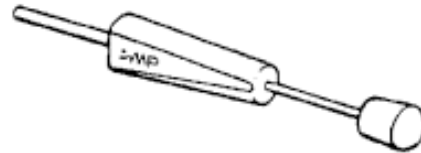


TOOLING

AMP Hand Crimping Tools and Applicators are available for applying crimp type contacts, also Insertion Tools and Extraction Tools assist in assembly and repair. Instruction Sheets and Applicator Instructions, describing tool operations, are packaged with the tool.



TYPICAL HAND CRIMPING TOOL



TYPE III+ AND SUBMINIATURE CONTACTS EXTRACTION TOOL (305183, IS 1216)



20 DF AND 20 DM CONTACTS INSERTION / EXTRACTION TOOL (91067-2, IS 7508)

**TSUNAMI MULTIPoint**

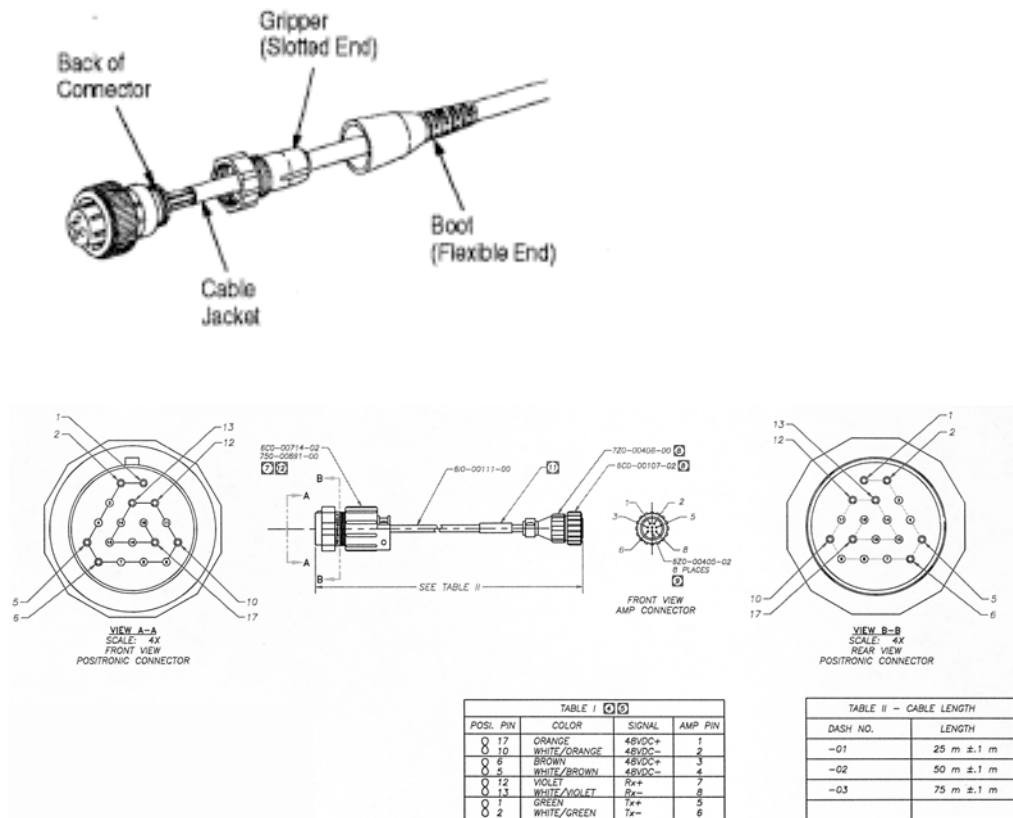
**INSTALLING FLEXIBLE STRAIN RELIEF BOOTS AND GRIPPERS**

Proceed as follows:

1. Install boot and gripper on cable before removing cable jacket. Slide boot onto cable flexible end first. Slide gripper onto cable slotted and first.
2. Crimp contacts to wires according to instructional material packaged with crimp tooling.
3. Insert contacts into housing according to instructions packaged with connector.
4. Thread gripper onto connector. Thread boot onto gripper until wire is tight. Do NOT over tighten.

*Over tightening of gripper on flexible boot can fracture boot.*

*Some threads on gripper may be exposed on larger diameter wire.*



**Figure 3-3: IDU to ODU cable**

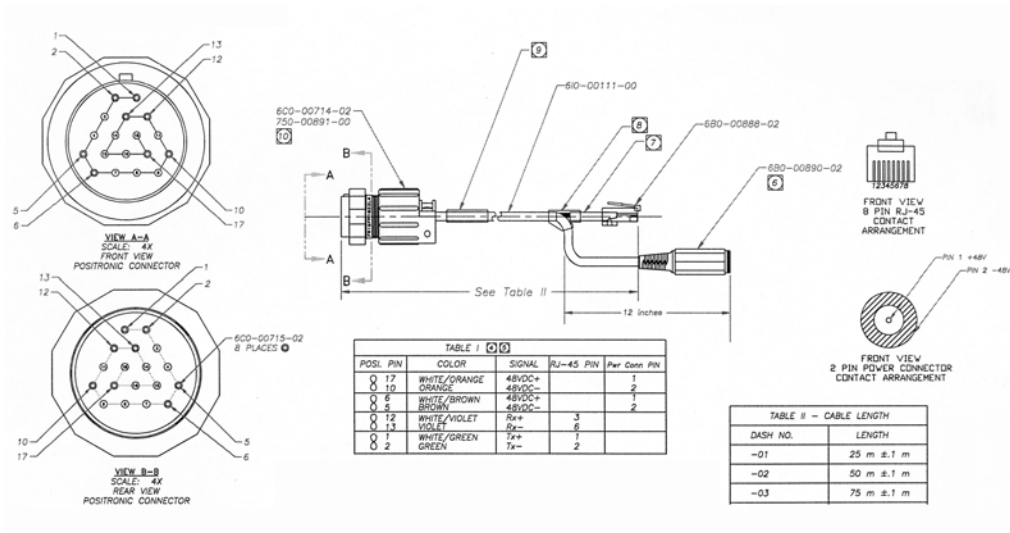


Figure 3-4: IDU to ODU cable w/separate power plug

### Alternative Method of Connection

Another method that is acceptable is to use what are called “jelly beans” or Telephone Wire Tap Connectors. These moisture resistant and easy to install devices have been used by the telephone industry for years both indoors and out (for this installation, recommendation is for using only indoors). These can be purchased at many electronic supply stores worldwide including Radio Shack (part #64-3081), Tandy or through most well stocked DIY stores. For this method, you will need eight (8) of these devices per cable.



Self-stripping tap connectors permit a continuous feed or loop without interruptions and let you splice wires without cutting any conductors. The connectors can be used with

Where you had to cut the cable for entry or egress, strip back the outer CAT5 cable jacket about two (2) inches on each side of the cut – do not strip the individual wires leaving bare copper! Into each 2-wire Tap Connector, push in the like colored wires from each cable end firmly and equally into the Tap. While holding the wires in firmly, squeeze the button with wide pliers to equally force the button into the Tap. If properly done, the button will now be flush with the rest of the Tap Connector body and the two wires will not pull out. Continue with the installation of seven (7) more of

## **T S U N A M I M U L T I P O I N T**

these Taps being sure that each wire from the ends of each severed cables match exactly in color per each Telephone-type Wire Tap Connector.

Refer to the table below that provides the details on each of the eight (8) wires that will need to be spliced from one cable to the like color on the other cable. After successfully installing the wire tap devices, the severed cable will carry the Ethernet and voltages necessary for operation.





## 4 Set-up Procedure

Please read this section completely before attempting to install any software, test or operate this system.

**Permanent damage to the equipment can result if directions are not followed exactly as provided.**

### Important Configuration Notes

#### NOTES:

- 1) When powering up with frame sync set to independent, the transmitter power is disabled for up to 10 seconds
- 2) When powering up with frame sync set to multi-sector, the transmitter power is disabled for up to 5.5 minutes
- 3) When changing frequency or inbound slot configurations with frame-sync set to independent, the transmitter power is disabled for 5 seconds.
- 4) When changing frequency or inbound slot configurations with frame-sync set to multi-sector, the transmitter power is disabled for 3 minutes.

The Base Station Configuration program is not ultimately intended to be a user's interface. However, this program does provide configuration controls for this particular system. The syntax of the data entry must be followed exactly as shown. When a string of characters is shown in this document with quotation marks around it (such as "IP"), do not type the quotation marks. When the letter "x" is shown within the quotation marks, this represents a number that the operator will select based on other factors. When the word (enter) is shown, this indicates pressing of the Enter (or Return) key on your keyboard. Wherever there are spaces shown in the syntax of a command, include these spaces. Commands are case sensitive.

## Unpacking the System

Pay close attention to how units are packed before unpacking.

SEE PHOTO BELOW AND NEXT PAGE FOR CLARIFICATION

The Base Station Unit (BSU), unpacking should be in the following steps:

- a. Remove power supply unit
- b. Remove loose cables and small mounting hardware in the bracket area
- c. Remove the top layer of foam being careful not to rip
- d. Remove large mounting bracket
- e. Remove BSU unit

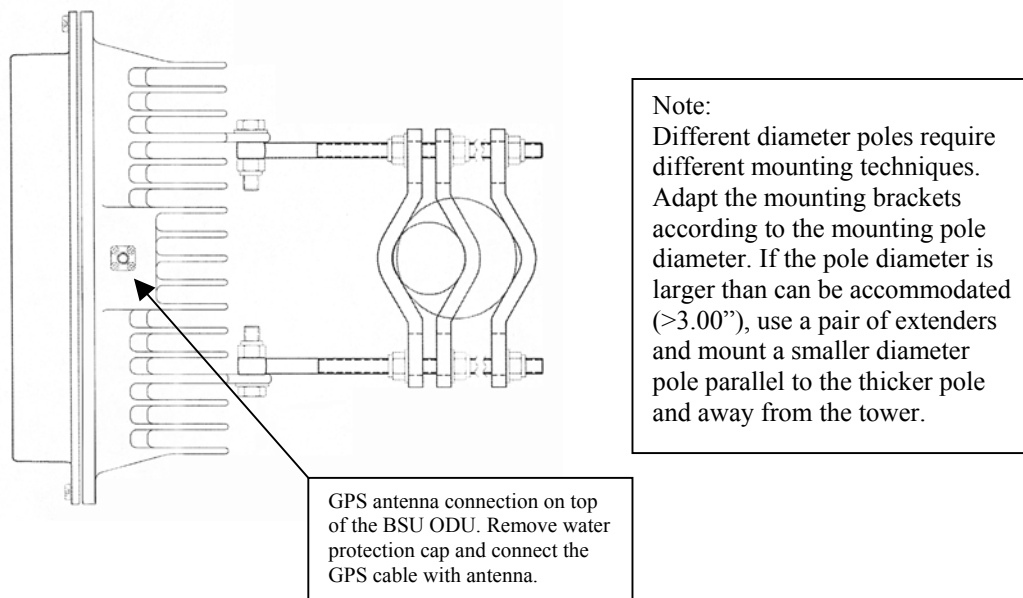


**Figure 4-1: Base Unit Kit**

## Mechanical Considerations – Mounting Units

The outside component of your Tsunami Multipoint Base Station Unit are designed to directly mount to 1-1/2 inch to 3 inch pole diameters (outer diameter).

For mounting directly to a proper size pole, first attach the bottom mounting bracket to the pole using the retainer as seen below while keeping the unit upright (lash to pole or keep hosting rope in place). Then attach the ODU to the pole using the upper mounting bracket, and lock into position by tightening the bottom bracket screws and the upper arm bolts using the supplied mounting nuts. To adjust the up/down tilt, move the arm nuts and bracket until at the right angel and then tighten all nuts as shown. See photos and diagrams below for detail. Connect the weatherproof circular connector from the cable from the power unit to the bottom of the ODU assembly.



**Figure 4-2: Base Station Unit ODU mounting detail**

### FLAT SURFACE MOUNTING

For mounting to a flat surface, attach mounting bracket to the SU using bolts supplied, and then mount to flat surface using your own hardware.

### GPS ANTENNA MOUNTING

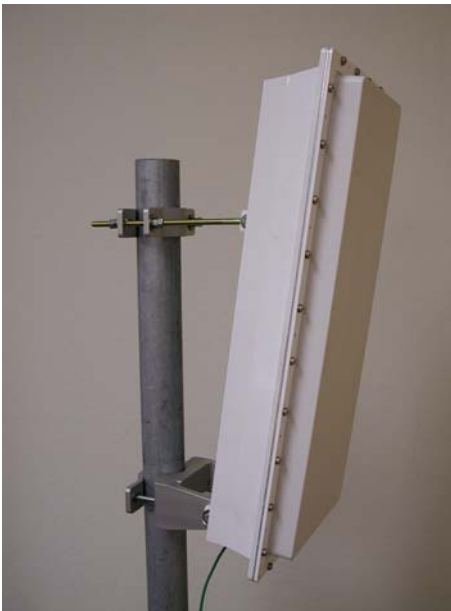
For operation with multiple base stations, the frame timing of all BSUs must be synchronized using GPS. The GPS antenna (small metal plate with black 2x2" antenna with thin cable) must be connected to the SMA connector on top of the ODU unit (see drawing above). Find a location nearby where the antenna plate can be mounted and secured with the black antenna bump up and the plate parallel to the earth/horizon. This small antenna needs to see as much of the sky as possible to

acquire at least one GPS satellite to extract timing signals for the ODU transmission synchronization.



**Figure 4-3: ODU with GPS antenna**

Each BSU ODU must have its GPS antenna attached and mounted as described above.

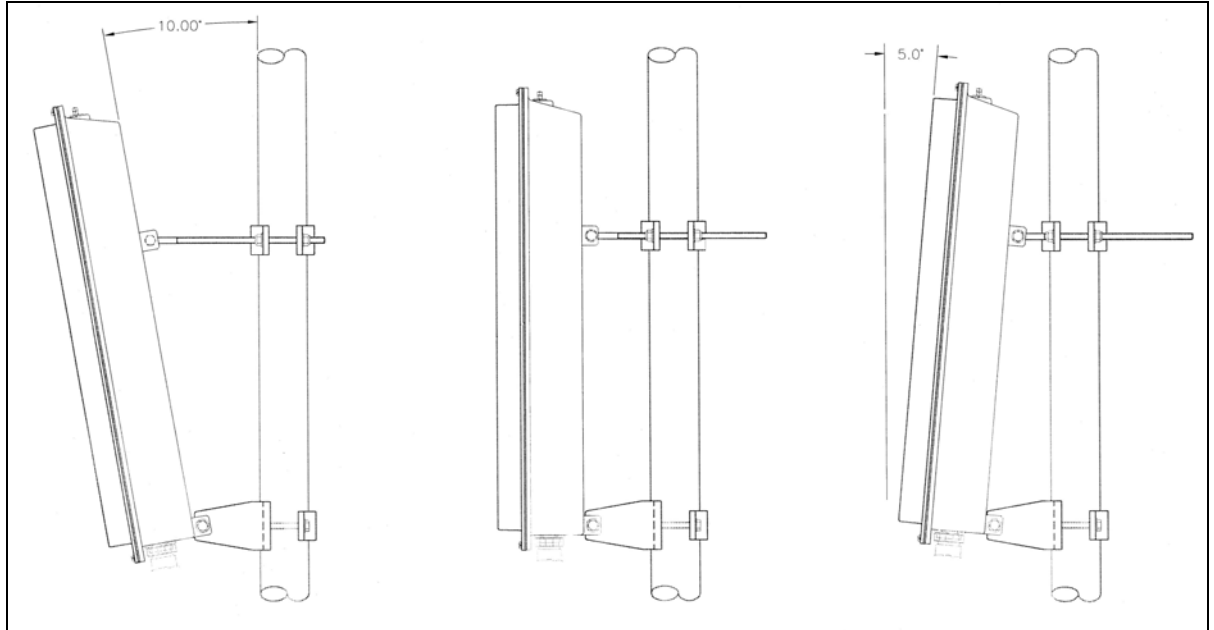


**Figure 4-4: Base Station ODU**

Connect the supplied cable between the ODU (pictured above) and the power unit mounted near your PC or network. The ODU cable to the inside power unit may be of two different styles (see Figures 2-12 and 2-13). Whichever cable, connect the ODU with the larger of the connectors by aligning the plastic slot and then hand-tighten the outside ring to secure and seal the connector to the ODU.

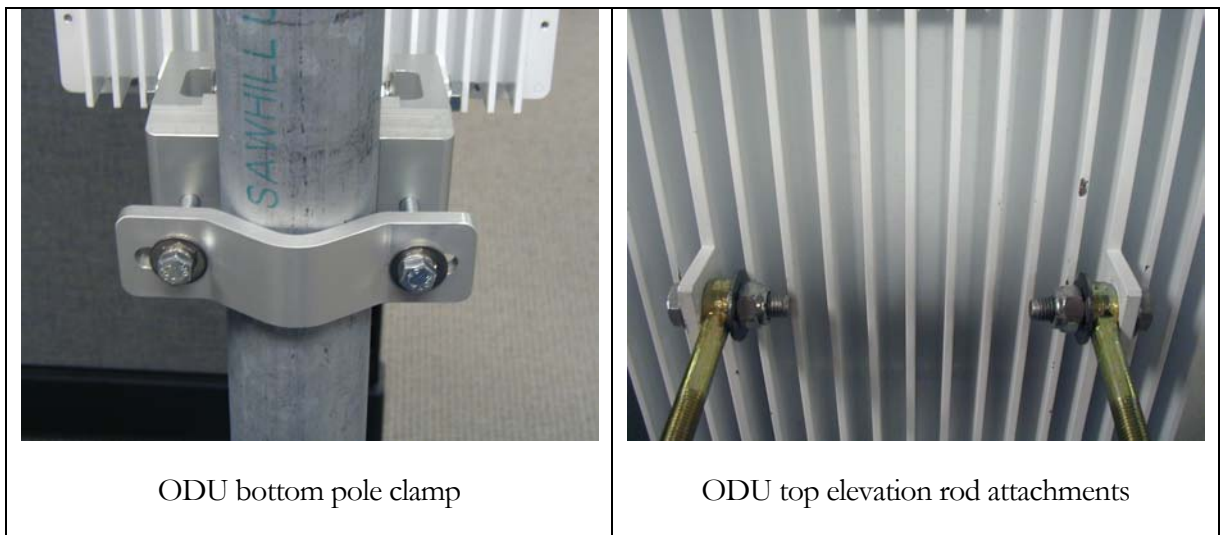
**TSUNAMI MULTIPPOINT**

Adjust the up/down tilt accordingly per the terrain and location of the SUs. Refer to the following Figure.



**Figure 4-5: Up and down tilt limits (-10 to +5 degrees)**

**Pictures helpful for installation**

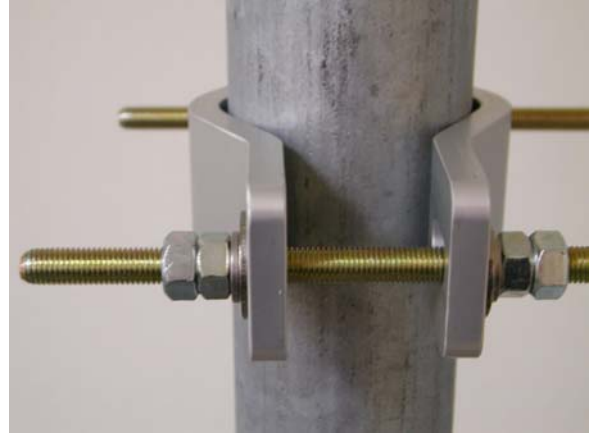


ODU bottom pole clamp

ODU top elevation rod attachments



ODU bottom bracket detail



ODU top bracket to pipe detail



ODU bottom bracket



ODU power and Ethernet connector



Power supply option with user Ethernet



ODU bottom showing ground/earth wiring

## **Software Installation**

Use the enclosed CD and install per instructions found on the CD in the readme.txt file.

The supplied BSU Configuration software will provide basic setup and operational capability; and is described in section 5. For managed system operation, consider acquiring the Wireless Manager.





## 5 Advanced Setup Commands

### Base Station Configuration Commands

#### Command to select frequency plan

Command: freqPlan <plan>

Example: freqPlan 4

Comment: The frequency plan assigned must lie between 4 to 6

Warning: This command will force the Base Station to reset automatically and come up with the new configuration.

#### Command to assign the operating frequency

Command: frequency <frequency>

Example: frequency a

Comment: The frequency entered should be between a and f and not exceed the range allowed under the current frequency plan. For example, under plan 4 the frequency selected should be between 'a' and 'd'.

Warning: This command will force the Base Station to reset automatically and come up with the new configuration

#### Command to assign the first inbound slot

Command: firstInboundSlot <slot number>

Example: firstInboundSlot 5

Warning: This command will force the Base Station to reset automatically and come up with the new configuration

#### Command to set the Base Station's Inbound Power Control margin, in dB.

Command: IPC <value>

Example: IPC 10

### Command to assign the number of reserved aloha channels

Command: `aloha <aloha channels>`  
 Example: `aloha 1`  
 Comment: At least one aloha channel must be assigned. The number of aloha channels cannot exceed 15.  
 Warning: This command will force the Base Station to reset automatically and come up with the new configuration

### Command to change the routing mode

Command: `routingMode <mode>`  
 Example: `routingMode 0`  
 Comment: The mode should be set to 0 for IP routing and 1 for bridging.  
 Warning: When the Base Station senses the routing mode has changed, it will restart and come up with the new routing mode and force all the SUs in its sector to restart.

### Command to turn the VLAN tagging on or off

Command: `setVLANTag <tag>`  
 Example: `setVLANTag 0`  
 Comment: Set the tag to 0 to turn VLAN tagging off and 1 to turn VLAN tagging on. VLAN tagging will take effect only in bridging mode

### Command to display the Base Station's configuration settings

Command: `dspsconf`  
 Comment: If `dspsconf?` is entered, all the available configuration commands and their syntax will be displayed

### Command to change the Base Station's IP address

Command: `setIP [IP address]`  
 Example: `setIP 192.168.20.10`  
 Comment: The Base Station console will display the Base Station's current IP address, if no IP address is entered.

### Command to change the Base Station's gateway IP address

Command: `gateway <gateway address>`  
 Example: `gateway 192.168.20.11`  
 Comment: The Base Station console will display the Base Station's current gateway address if no gateway address is entered.

### **Command to change the Base Station's id**

Command: setID <terminal id>  
 Example: setID 2  
 Comment: If no parameter is entered the Base Station's existing id will be displayed.

### **Command to set the Base Station's subnet mask**

Command: setSubnet < subnet mask>  
 Example: setSubnet 255.255.254.0  
 Comment: The Base Station console will display the Base Station's current subnet mask, if no subnet mask is entered.

### **Command to activate range checking for all SUs associated with the Base Station**

Command: rangeSecurity <tag>  
 Example: rangeSecurity 0  
 Comment: Set the tag to 0 to turn range checking off and 1 to turn range checking ON. If the range checking is on, and a SU is trying to enter the net, the Base Station will check the range value reported by the SU. If this is the first time the SU tries to enter the net, its range will be stored in the Base Station's flash memory for future reference. If the SU has entered the net before and its reported range does not match with what has been stored in the flash memory, the SU will be denied net entry and an alarm will be sent to the Ethernet Console and the Wireless Manager.

### **Command to turn the Base Station's transmitter on or off.**

Command: txPower <tag>  
 Example: txPower 0  
 Comment: If tag is 0 the transmitter will be turned off. If the tag is 1 the transmitter will be turned on.

### **Command to turn the Base Station's transmit power level.**

Command: txPowerLevel <level>  
 Example: txPowerLevel 17  
 Comment: The transmit power level should be between 6 and 17 dBm.

### **Command to automatically turn on or off the transmitter upon power up**

Command: txPowerAutoEnable <tag>  
 Example: txPowerAutoEnable 0  
 Comment: If tag is 1 the transmitter will be turned on automatically when the Base Station power up.

### Command to show the Base Station's arp table

Command: arp

### Command to ping a device connected to the BSU

Command: ping <IP address>

Comment: This command allows the operator to ping a device with the specified IP address. For this to work, the device must be located on the Base Station side. That is, the operator cannot ping a device connected to a Subscriber Unit from the Base Station console.

### Command to turn data squelch on or off

Command: dataSquelch <tag>

Example: dataSquelch 0

Comment: If tag is 0 data squelch will be turned off. Otherwise, it will be turned on.

### Command to display the firmware version

Command: version

Example: version

Comment: Response is to show the starting banner.

### Command to display available commands.

Command: help

Example: help

Comment: Response is to list all available commands and their usage.

### Command to set frame synchronization mode

Command: setFrameSync <mode>

Example: setFrameSync 1

Comment: Mode 0: Multi Sector (If more than one BSU in a cell site, using GPS timing is necessary and requires that the nearby BSUs are in time synchronization)

Mode 1: Independent (Only one BSU in use, so time synchronization is not necessary)

## SU Configuration Commands

### Command to add a Subscriber Unit to the Base Station's database.

Command: addSU <eth0><eth1><eth2><eth3><eth4><eth5><terminal ID>  
 Example: addSU f0f0f0f0f021  
 Comment: <eth0> to <eth5> is the Ethernet address assigned to the Subscriber Unit

### Command to remove a Subscriber Unit from the Base Station database.

Command: removeSU <terminal ID>  
 Example: removeSU 1

### Command to assign a VLAN ID to a Subscriber Unit.

Command: setSUVLAN <terminal ID><VLAN ID>  
 Example: setSUVLAN 1 2

### Command to assign a subnet mask to a Subscriber Unit.

Command: setSUSubnet <terminal ID><subnet mask>  
 Example: setSUSubnet 1 255.255.255.0

### Command to set the SU's IP address.

Command: setSUIP <terminal ID><IP address>  
 Example: setSUIP 1 192.168.20.10  
 Comment: When an SU is created, its IP address will be defaulted to the same as the Base Station's IP address.

### Command to display a Subscriber Unit's configuration parameters and traffic statistics

Command: dspSU <terminal ID>  
 Example: dspSU 1  
 Comment: Terminal ID is an optional parameter. If terminal ID is not entered, then all Subscriber Units in the Base Station's database will be displayed.

### Command to display subscribe units that have entered the network.

Command: dspActiveSU

### Command to add a static IP address of PC attached to a Subscriber Unit.

Command: addSUIP <terminal ID><IP address>  
 Example: addSUIP 1 192.168.20.10  
 Comment: Up to 5 static IP addresses can be entered. Once the limit has been reached, the following warning message will be displayed "Cannot add any more static IP address". In that case

an existing static IP addresses has to be deleted before a new one can be added. The static IP addresses associated with the SU can be displayed using the dspSU command.

**Command to remove a static IP address from a Subscriber Unit.**

Command: removeSUIP <terminal ID><IP address>  
 Example: removeSUIP 1 192.168.20.10

**Command to disable a Subscriber Unit.**

Command: disableSU <terminal ID>  
 Example: disableSU 1  
 Comment: This command will put the SU into the listen only mode. The SU will continue to receive the outbound control messages, but will not attempt to receive or transmit user data in the downlink and uplink direction respectively.

**Command to enable a Subscriber Unit**

Command: enableSU <terminal ID>  
 Example: enableSU 1  
 Comment: This command will cause the SU that has been disabled to exit the listen only mode, restart itself and reenter the net.

**Command to set the gateway address of a Subscriber Unit.**

Command: setSUGateway <terminal ID><gateway>  
 Example: setSUGateway 1 192.168.20.10  
 Comment: If no gateway is present the gateway address should be set to 0.

**Command to set the IP Filter mode of a Subscriber Unit**

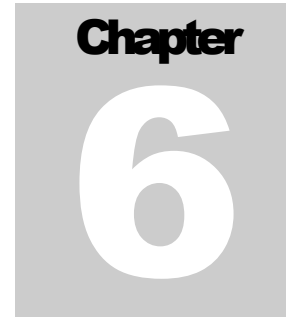
Command: setSUFilter <terminal ID><access mode>  
 Example: setSUFilter 1 0  
 Comment: Filter mode 0: “Restricted” - This is a restricted access and only PCs with a static IP address assigned by the Base Station or an IP address obtained via DHCP will be allowed to access the wireless network.  
 Filter mode 1: “Subnet” - This mode allows only PCs that has the same subnet address as the Subscriber Unit to access the wireless network  
 Filter mode 2: “Local” - This mode allows all PCs connected to the Subscriber Unit’s LAN to access the network.  
 Filter mode 3: “Open” - This mode allows any PCs, either locally connected to the Subscriber Unit or remotely connected to the Subscriber Unit via a router to access the network (not presently implemented).

setSUFilter <termid> <mode>" should be list the choices for <mode> as 0, 1, 2 or 3 instead of restricted, local, subnet, and open. This will also need to be addressed in the BSU software help menu, which will require a revision of this too. Currently, mode 3 doesn't work and is likely to require a firmware change in either the BSU or SU (to be determined).









## 6 Troubleshooting

### Regular Maintenance

There is no regular maintenance required except to keep the surfaces free from debris, dirt and dust.

### Problem – Solution

#### Problem:

If the BSU operator sees "Fault: Multi-sector mode but no GPS 1PPS messages detected - restarting GPS."

#### Possible Causes:

- ✓ Means that the GPS receiver is not receiving a signal from at least 4 satellites because of signal blockage or interference.

#### Recommended

The installer should relocate the antenna

### Unsolicited Base Station messages

“100 Terminal %i and terminal %i have same Ethernet address %x.%x.%x.%x.%x.%x\n”

Explanation: Two different SUs have the same Ethernet address stored in the BS's database

"101 Terminal id %i has default Ethernet address deadbecafe"

Explanation: An SU's Ethernet address is not defined in the database

"103 DB check completed"

Explanation: Database verification is completed

"104 Save NV Networking Parameters"

Explanation: Save networking parameters into the database

"105 Save NV Calibration Parametersn"

"106 Save NV Netentry Parameters"

"107 Save NV configuration Parameters"

Explanation: NV parameters are being saved into the flash memory

"108 NV updated"

Explanation: Update of flash memory has been completed

"109 Prepare to warm start"

"110 No valid data found in config sector... default NV values are used"

"111 No valid data found in calibration sector ... default NV values are used"

"112 No valid data found in calibration sector ... default NV values are used"

"113 No valid data found in network sector ... default NV values are used"

**TSUNAMI MULTIPPOINT**

"114 Completed flash sector verification"

# Repair and Return Instructions and Policy Statement

Should it become necessary to send a product(s) in for repair, please call 408-542-5390 ext. 2 (technical support) or you may email your request to [support@wmux.com](mailto:support@wmux.com), Monday through Friday 8:00 am – 5:00 pm PST, excluding U.S. holidays.

Below is a list of information needed prior to the issue of an RMA#:

- A service order number, assigned by a Western Multiplex technical support engineer.
- Model and serial # of each unit.
- A validated failure description of each unit. Our technical assistance personnel can assist in failure validation.
- Company name, billing, and shipping address.
- Contact person name and phone #.
- A purchase order # if the unit is out of warranty.
- A hardcopy of the PO# is required for any repair cost greater than \$1,000.00. Please fax to 408-542-3375 prior to the return of the unit.

For other warranty details please refer to the warranty page in the first section of the manual.

Policies associated with the return of product:

- RMA numbers are assigned within 24 hours of request or 24 hours after all information is made available to WMUX.
- WMUX makes every effort to ensure a 30 day turnaround time from receipt of product to the shipment of product back to the customer.
- Proper and adequate packaging must be used for shipments. When available the original packing boxes should be used.
- The RMA number must reside on the outside of the box and referenced on shipping paperwork. Product delivered without proper identification will either be shipped back to originator or delivered to a discrepancy area until proper identification can be made. This will cause delay in receipt of product into WMUX.
- No more than 10 products can be returned at any one time.

Other available services:

- Expediting fees and advanced exchange options are available at per incident rates and are subject to inventory. Options and quotes can be given to you at the time of request.

# INDEX

## **A**

Accessories .....	3-9
Antennas .....	3-5
ARP .....	2-7

## **B**

Bridging .....	2-11
Bridging mode .....	2-2
Burst rate .....	3-7

## **C**

Cables .....	3-14
<b>CLOS</b> .....	<b>3-7</b>
Commands .....	5-1
Configuration .....	3-8, 4-1, 5-1
Crimping .....	3-11

## **D**

Dimensions .....	3-9
<b>Distance</b> .....	<b>3-7</b>

## **E**

Electrical .....	3-8
------------------	-----

## **F**

Filters .....	2-1, 2-6
Fresnel .....	3-7

## **G**

Gateway .....	2-5
GPS antenna .....	4-3

## **I**

Installation .....	3-1, 3-9, 4-5
Interference .....	3-3
IP routing .....	2-5, 2-11

## **L**

Lightning .....	3-3
Link budget .....	3-6

## **M**

Maintenance .....	6-1
Mechanical .....	4-3
MIB .....	3-8
Mounting .....	4-3

## **N**

Network .....	2-1, 2-8, 2-12
<b>NLOS</b> .....	<b>3-7</b>

## **P**

Pictures .....	4-5
Planning .....	3-1
Problem – solution .....	6-1

## **R**

Rain .....	3-2
Repair .....	6-4

## **S**

Safety instructions .....	1-4
SNMP .....	3-8
Software .....	4-7
Specifications .....	3-7

## **T**

Tilt .....	4-5
Tools .....	13
Tower .....	3-6
Troubleshooting .....	6-1
Tx power .....	3-7

## **U**

Unpacking .....	4-2
-----------------	-----

## **V**

VLAN .....	2-3, 2-4
------------	----------

## **W**

Warranty .....	ii
Weather .....	3-2